MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

EX DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

YOUNITED S.A., SEDE SECONDARIA ITALIANA

INDICE

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/2001

1.1. Caratteristiche fondamentali ed ambito di applicazione.

Con l'entrata in vigore del Decreto, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" è stata introdotta nell'ordinamento italiano una responsabilità in sede penale (formalmente qualificata come responsabilità "amministrativa") degli enti.

Il legislatore italiano si è in questo modo conformato ad una serie di provvedimenti comunitari ed internazionali che richiedevano una maggiore responsabilità degli enti che fossero coinvolti nella commissione di alcuni tipi di illeciti aventi rilevanza penale, soprattutto in materia finanziaria.

La normativa in questione prevede una responsabilità degli enti che si aggiunge a quella delle persone fisiche che hanno materialmente realizzato l'illecito e che sorge qualora determinati reati o illeciti amministrativi siano commessi nell'interesse o a vantaggio dell'ente, in Italia o all'estero, da parte di:

- persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società, o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da parte di persone che esercitano anche di fatto la gestione e il controllo dell'ente (i c.d. soggetti apicali);
- persone sottoposte alla direzione o alla vigilanza di uno dei predetti soggetti apicali.

Ai sensi del Decreto, i Destinatari della normativa sono: gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica. Sono espressamente sottratti all'ambito di applicazione del Decreto: lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici, nonché gli enti che svolgono funzioni di rilievo costituzionale.

Con riferimento ai soggetti italiani, il Decreto si applica in relazione sia a reati ed illeciti amministrativi commessi in Italia sia a quelli commessi all'estero, salvo che nei confronti degli stessi non proceda lo Stato in cui è stato commesso il reato e purché l'ente abbia nel territorio dello Stato italiano la sede principale.

Riguardo gli enti giuridici di diritto straniero operanti in Italia, anche per mezzo di succursali, la principale tesi giurisprudenziale, avallata costantemente sin dalla decisione del 2004 sul caso Siemens AG[1], ammette l'applicabilità del D. Lgs. 231/2001 anche ad essi. Ciò sulla base del principio di imperatività della norma penale, a ragione del quale il semplice fatto di operare in Italia comporta l'obbligo di rispettarne la legge, indipendentemente dall'esistenza nel Paese di appartenenza della società di norme che regolino la stessa materia in modo analogo. Dunque, nel momento in cui l'ente estero decide di operare in Italia, sul medesimo grava l'onere di attivarsi e di uniformarsi alle previsioni normative

italiane; diversamente, l'ente si attribuirebbe una sorta di auto esenzione dalla normativa italiana, in contrasto con il principio di territorialità della legge e, in particolare, con l'art. 3 del codice penale.
Altro argomento posto a supporto della suesposta tesi è tratto dal disposto dell'art. 36 del D. Lgs. 231/2001, il quale sancisce che il giudice penale competente in ordine al reato presupposto è altresì competente a conoscere anche dell'illecito amministrativo dell'ente.

Le fattispecie di reato ed illecito amministrativo suscettibili di configurare la responsabilità amministrativa sono soltanto quelle espressamente indicate dal legislatore all'interno del Decreto, che, al momento dell'emanazione, contemplava solo alcuni reati nei confronti della Pubblica Amministrazione. Tuttavia, il legislatore, anche in applicazione di successive direttive comunitarie, ha nel corso degli anni notevolmente ampliato il catalogo dei Reati, che oggi comprende, in particolare:

a) **reati contro la Pubblica Amministrazione** (artt. 24 e 25[2]);
b) **delitti informatici e trattamento illecito dei dati** (art. 24-*bis*);
c) **delitti di criminalità organizzata** (art. 24-*ter*);
d) **delitti in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** *(art. 25- bis);*
e) **delitti contro l'industria e il commercio** (art. 25-*bis.1*);
f) **reati societari e corruzione tra privati** (art. 25-*ter*);
g) **delitti con finalità di terrorismo o di eversione dell'ordine democratico** *(art. 25-quater);*
h) **pratiche di mutilazione degli organi genitali femminili** (art. 25-
i) *quater*.1);
j) **delitti contro la personalità individuale** (art. 25-*quinquies*);
k) **reati e illeciti amministrativi di abuso di mercato** (art. 25-*sexies*);
l) **reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (art. 25-*octies*);
m) **delitti in materia di strumenti di pagamento diversi dai contanti** (art. 25-*octies*.1)
n) **delitti in materia di violazione del diritto d'autore** (art. 25-*novies*);
o) **induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** *(art. 25-decies);*
p) **reati ambientali** (art. 25-*undecies*);
q) **impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (art. 25-duodecies);
r) **razzismo e xenofobia** (art. 25-*terdecies*);
s) **frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati** *(art. 25-quaterdecies);*
t) **reati tributari** (art. 25-*quinquiesdecies*);
u) **contrabbando** (art. 25-*sexiesdecies*);
v) **delitti contro il patrimonio culturale** (art. 25-*septiesdecies*);
w) **riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici** *(25 duodevicies)*
x) **reati transnazionali** (richiamati dall'art. 10 della legge 16 marzo 2006, n. 146, di seguito, la "**Legge 146/2006**").

Non si può escludere, in futuro, l'inserimento di nuovi titoli di reato o illecito amministrativo presupposto nel Decreto.

1.2. Il modello organizzativo come forma di esonero dalla responsabilità

Ai sensi del Decreto Legislativo 8 giugno 2001, n. 231 (di seguito, anche "il **Decreto**"), l'ente non risponde per gli illeciti amministrativi dipendenti da reato commessi da soggetti in posizione apicale, qualora riesca a dimostrare congiuntamente che:

- ha adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi;
- ha affidato a un organismo dell'ente, dotato di autonomi poteri di iniziativa e controllo, il compito di vigilare sul funzionamento e sull'osservanza del modello, nonché di curarne l'aggiornamento;
- gli autori del reato hanno eluso fraudolentemente il modello medesimo;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Con riferimento ai reati commessi da soggetti sottoposti all'altrui direzione o vigilanza, l'ente risponde solo qualora la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. È in ogni caso esclusa la responsabilità dell'ente se quest'ultimo ha adottato ed efficacemente attuato, prima della commissione del fatto, un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto, inoltre, stabilisce che i modelli di organizzazione, gestione e controllo devono rispondere alle seguenti esigenze:

a. individuare le attività nel cui ambito possono essere commessi i reati;
b. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
c. individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
d. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del modello;
e. introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

In conformità a tale disposizione Younited, nella predisposizione del presente Modello, si è ispirata alle linee guida emanate dall'AIBE e dall'ABI, nonché a quelle elaborate da Confindustria ("**Linee Guida**").

Occorre, tuttavia, precisare che le indicazioni contenute nelle Linee Guida rappresentano un mero quadro di riferimento cui gli enti possono liberamente ispirarsi ai fini dell'adozione del proprio modello di organizzazione, gestione e controllo.

Il modello organizzativo e gestionale deve, inoltre, prevedere un efficace

sistema di controllo volto a garantire la corretta attuazione del modello stesso e il mantenimento nel tempo delle condizioni di idoneità delle misure adottate.
Il riesame e l'eventuale aggiornamento del modello devono essere effettuati ogniqualvolta:

- emergano significative violazioni delle disposizioni normative in materia di salute e sicurezza sul lavoro;
- si verifichino mutamenti nell'organizzazione aziendale o nelle attività svolte, ovvero intervengano sviluppi scientifici o tecnologici rilevanti.

1.3. L'apparato sanzionatorio

Il Decreto prevede che agli enti possano essere applicate sanzioni pecuniarie e sanzioni interdittive. In particolare, nel settore bancario e finanziario è previsto l'intervento della Banca d'Italia e della Consob sia con un ruolo di collaborazione con il pubblico ministero e con il giudice del procedimento penale, sia con l'incarico di porre in essere l'esecuzione delle eventuali sanzioni interdittive disposte nei confronti di una banca/impresa di investimento, di cui all'art. 9, comma 2, del Decreto (lettere a) – interdizione dall'esercizio dell'attività e b) – sospensione o revoca dall'autorizzazione).Le sanzioni pecuniarie si applicano ogniqualvolta un ente commetta uno degli illeciti previsti dal Decreto, mentre quelle interdittive possono essere applicate solo in relazione ai Reati per i quali sono espressamente previste dal Decreto, qualora ricorra almeno una delle seguenti condizioni:

- l'ente ha tratto dal Reato un profitto di rilevante entità ed il reato è stato commesso (i) da soggetti in posizione apicale, ovvero (ii) da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del Reato è stata determinata o agevolata da gravi carenze organizzative;
- in caso di reiterazione degli illeciti.

Le sanzioni pecuniarie vengono applicate per quote in un numero non inferiore a cento né superiore a mille (l'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di tre milioni). Ai fini della quantificazione delle sanzioni pecuniarie il giudice deve tenere conto:

- della gravità del fatto;
- del grado di responsabilità dell'ente;
- dell'attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- delle condizioni economiche e patrimoniali dell'ente.

Le sanzioni interdittive applicabili agli enti ai sensi del Decreto sono:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di concludere contratti con la pubblica amministrazione, salvo che per ottenere le prestazioni di pubblico servizio;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nella revoca

di quelli già concessi;
- il divieto di pubblicizzare beni e servizi.

Il tipo e la durata (che può variare da tre mesi a due anni) delle sanzioni interdittive sono stabiliti dal giudice sulla base dei criteri indicati per la commisurazione delle sanzioni pecuniarie. Il Decreto prevede, inoltre, la possibilità di applicare alcune sanzioni in via definitiva (quindi superando il limite massimo di durata di due anni), qualora si verifichino determinati eventi considerati particolarmente gravi dal legislatore. Se necessario, le sanzioni interdittive possono essere applicate anche congiuntamente.

Con specifico riferimento al settore bancario, in virtù dell'art. 97-*bis*, quarto comma del Testo Unico Bancario, le sanzioni interdittive di cui alle lettere a) e b) dell'art. 9, secondo comma del Decreto (interdizione dall'esercizio dell'attività e sospensione o revoca dell'autorizzazione) non possono essere applicate in via cautelare alle banche. La stessa norma stabilisce, altresì, un flusso informativo tra il Pubblico Ministero che iscrive nel registro delle notizie di reato un illecito amministrativo a carico di una banca e la Banca d'Italia e la Consob, le quali possono essere sentite nel corso del procedimento ed hanno, in ogni caso, la facoltà di presentare relazioni scritte[4].

Oltre alle predette sanzioni, il Decreto prevede che, ove sia comminata una sanzione interdittiva, venga sempre disposta la confisca del prezzo o del profitto del Reato (ovvero del relativo equivalente in termini monetari), nonché la pubblicazione della sentenza di condanna.

2. L'APPROCCIO METODOLOGICO ADOTTATO

2.1 La scelta della Sede Secondaria italiana

Correttezza e trasparenza nella conduzione dei propri affari rappresentano una componente dei valori e della politica aziendale di Younited, contribuendo a tutelare l'immagine di quest'ultima e le aspettative dei suoi clienti.

La Sede Secondaria ha dunque deciso di adottare un proprio Modello e di attivarsi in ogni modo per garantirne il rispetto, procedendo ad una mappatura analitica di tutte le attività che vengono effettuate dalla succursale italiana di Younited S.A.

2.2 I Presupposti

La Sede Secondaria italiana di Younited S.A. ("**Sede Secondaria**" o "**Succursale**"), in ragione della sua appartenenza ad un gruppo internazionale, dispone già di un articolato sistema di strumenti organizzativi e di controllo, volti a tutelare i predetti valori, che contengono già importanti presidi per la prevenzione dei Reati.

Precisamente:

- Sistema dei poteri che, attraverso gli opportuni strumenti (organigrammi, deleghe di funzioni, disposizioni organizzative, procedure, procure, ecc.) stabilisce i poteri di rappresentanza e definisce formalmente i ruoli e le responsabilità, le linee gerarchiche e i riporti funzionali delle unità organizzative.
- Sistema di controlli interni che coinvolge con ruoli diversi il management, le funzioni di controllo e le singole unità organizzative attraverso la previsione di controlli di linea che garantiscono la corretta esecuzione delle operazioni e meccanismi di monitoraggio.
- Codice Etico (Allegato A) che definisce i principi etici generali di condotta del Gruppo a cui tutto il personale, nonché i collaboratori ed i consulenti esterni del Gruppo devono ispirarsi, nello svolgimento delle proprie attività sociali.
- Un sistema strutturato e organico di Policy e Procedure richiamate nelle parti Speciali del Modello.
- Sistemi di comunicazione interna e formazione del personale.

Tali strumenti, pur non essendo riportati dettagliatamente nel Modello costituiscono un prezioso strumento per presidiare comportamenti illeciti e vanno ad integrare quanto previsto nel Modello. Tutti i Destinatari sono tenuti a rispettare i menzionati presidi, in relazione al tipo di rapporto in essere con la Sede Secondaria.

L'elenco dei documenti sopra richiamati è contenuto nelle matrici di rischio e nelle schede di Gap Analysis, disponibili presso l'archivio dell'OdV.

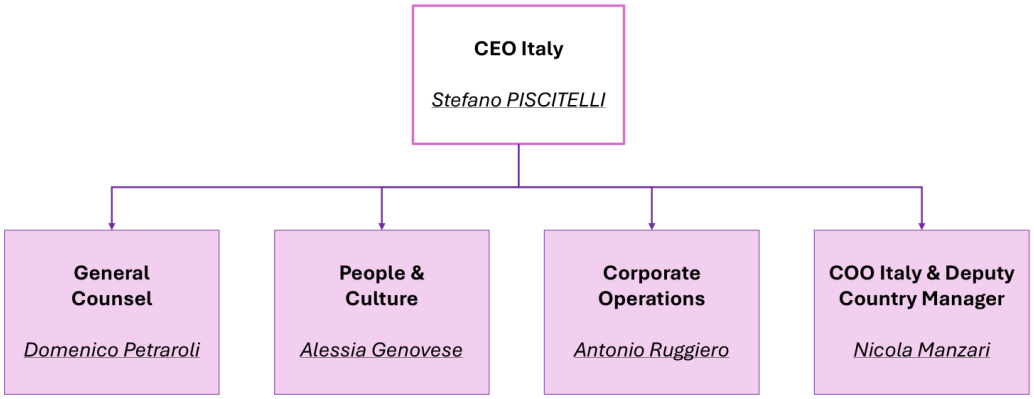
La parte del Modello Organizzativo relativa alla Succursale italiana è stata predisposta tenendo conto della *business combination* realizzata tra Younited S.A. e Younited Financial S.A.(già Iris Financial), società di diritto lussemburghese che, alla data di predisposizione del presente documento, è quotata presso i mercati Euronext di Parigi e Amsterdam, come da informative e documentazione disponibili nella sezione "*investor relations*" del sito istituzionale di Younited.

In tale contesto, si sottolinea che, in qualità di succursale italiana di una banca francese, è necessario dotarsi di un presidio di controllo dei rischi conforme non solo alla normativa bancaria e finanziaria di riferimento, ma anche alle nuove fattispecie di reato presupposto introdotte dal D.Lgs. 231/2001, applicabili alle società emittenti strumenti finanziari quotati.

2.3 Gli strumenti di governance adottati

Alla data di predisposizione del presente documento, la Sede Secondaria italiana conta 71 dipendenti, numero destinato evolvere in relazione alle stime di crescita del volume d'affari.

L'organigramma della Succursale, aggiornato al 15 settembre 2025, è così rappresentato:



Lo sviluppo commerciale è un'area nella quale la Sede Secondaria gode di ampia autonomia decisionale.

Le decisioni strategiche finali restano in ogni caso sottoposte alla validazione dei Comitati di Gruppo (es. Comitato Esecutivo e Comitato Rischi) che periodicamente valutano ogni singola proposta avanzata dalla Succursale.

Al **CEO Italy** compete l'intero coordinamento del team italiano. In qualità di "Country Manager" per l'Italia, il CEO Italy ha difatti tutti i poteri e le responsabilità richiesti al fine di svolgere i suoi compiti, inclusi i poteri di decisione, prevenzione, controllo e sanzionatori. Il CEO Italy ha piena libertà nell'adozione di tutte le misure necessarie, anche ove non siano urgenti, e di qualsiasi provvedimento disciplinare immediato che ritenga necessario nei confronti dei dipendenti della Sede Secondaria. Nell'ambito del Gruppo, il CEO Italy riveste il ruolo di membro del Comitato Esecutivo di Gruppo.
A diretto riporto del CEO Italy è posto il General Counsel Italy, che ricopre altresì, il ruolo di Responsabile Compliance e Antiriciclaggio della Succursale Italiana. In tale contesto, la responsabilità delle Segnalazioni di Operazioni Sospette ai sensi della normativa applicabile è stata delegata dal CEO Italy a una risorsa specializzata della Succursale, a diretto riporto del General Counsel Italy.

In merito ai principali elementi dell'organizzazione a livello di Gruppo si riporta quanto segue.

Il **Consiglio di Sorveglianza** ("***Supervisory Board***") si avvale di 3 comitati dedicati per il rischio, la revisione contabile e la remunerazione. Tali comitati sono composti da azionisti chiave. I dipendenti di Younited S.A. selezionati sono invitati a partecipare ad alcune commissioni quando necessario. La funzione centralizzata del rischio copre tutti i Paesi in modo da assicurare un presidio dei rischi fortemente accentrato e indipendente dalle diverse aree di attività.

Anche il **Consiglio di Gestione** ("***Directoire***") si avvale di comitati dedicati in

funzione delle rispettive competenze, q, che possono prevedere la partecipazione mirata di membri del management. In particolare, il Consiglio di Gestione si avvale di un Comitato Esecutivo ("*ExCo*") composto dal *top management* di Casa madre e dai CEO delle *Business Unit*. I principali ambiti di supervisione e indirizzo riguardano:

- strategia, organizzazione e studi dettagliati per ogni *Business Unit*;
- analisi approfondita degli indicatori di performance chiave;
- definizione della strategia per l'attività operativa, in linea con la propensione al rischio e le relative politiche di Gruppo;
- valutazione e gestione degli aspetti operativi.

2.4 Le caratteristiche salienti del sistema dei controlli interni

Il sistema dei controlli interni di Younited S.A. si articola in tre "linee di difesa", che mirano a garantire un controllo costante e strutturato sull'attività e sui rischi cui Younited, compresa la Sede Secondaria, è esposta.

La prima linea è incentrata su un controllo dal taglio maggiormente operativo, affidato alle strutture di "linea" e ai rispettivi *manager*, che monitorano l'attività nel continuo e possono segnalare eventuali anomalie nei processi e/o dei controlli in vigore. Tale monitoraggio comprende i cosiddetti **controlli di primo livello**, i quali, seguendo le linee guida dettate dal piano di controlli interni, si sostanziano in una serie di verifiche *ad hoc* sulla rispettiva propria area di competenza per verificare la completa aderenza alla normativa di processo in vigore. Tali controlli sono periodicamente comunicati alla funzione incaricata dei controlli interni.

La seconda linea di controllo è affidata alle strutture non operative (i.e. funzioni di controllo di secondo livello quali la funzione di conformità e di *risk management*), le quali, oltre a definire modalità e pianificazione dei controlli vigenti, ne monitorano costantemente i risultati, valutando le azioni di miglioramento ritenute necessarie.

La terza linea di difesa è presidiata dalla funzione di *Internal Audit*, che è attualmente affidata a una società terza di consulenza, selezionata in base a criteri di competenza, indipendenza e comprovata esperienza in materia di controllo interno e compliance normativa.

Tale assetto consente di garantire un'adeguata separazione dalle funzioni operative e il rispetto del principio di terzietà, in coerenza con le Linee Guida di Banca d'Italia in materia di controlli interni, nonché con i requisiti richiesti dal D.Lgs. 231/2001 in termini di efficacia del sistema dei presidi e di autonomia della funzione di verifica.

L'attività di controllo interno sulla conformità delle operazioni ai processi ed alle procedure all'interno della Sede Secondaria ha un duplice raggio di applicazione:

- La Casa Madre ha piena autonomia e discrezione nell'implementazione dei controlli sulla globalità della Sede Secondaria;

- La Sede Secondaria italiana provvede, mediante la funzione incaricata dei

controlli interni della Succursale italiana, attualmente incardinata presso l'area General Counsel Italy, all'assolvimento dei controlli di secondo livello sulle aree interne presenti nell'organigramma.

I controlli interni vengono effettuati sotto la supervisione della funzione Internal Control della Casa Madre per valutare su base periodica, non solo la conformità alla normativa italiana, ma anche la conformità della Sede Secondaria alle linee guida dell'autorità del Paese di origine ACPR ("*Autorité de controle prudentiel et de résolution*").

Mediante il controllo svolto annualmente, in particolare, la Younited S.A. mira ad esaminare eventuali aree di potenziale miglioramento o di disfunzione al fine di proporre azioni correttive o migliorative.

La Sede Secondaria fornisce a sua volta alla Younited S.A. tempestivo riscontro rispetto alla sua attività di controllo interno di secondo livello.

La funzione incaricata dei controlli interni di secondo livello della Succursale annualmente partecipa alla redazione di un piano dell'attività "**Internal Control Plan**", che verrà svolta nel corso dell'anno, dettagliando:

- Controlli;
- Aree che interesseranno;
- Le modalità con cui verranno effettuati.

In sede di predisposizione dell'Internal Control Plan, le funzioni preposte tengono in considerazione anche gli esiti della valutazione dei rischi cui Younited S.A. è complessivamente esposta (*Risk & Control Self-Assesment* di Gruppo), che si svolge su base annuale secondo la pianificazione della Casa Madre e con la supervisione dalla funzione di *Enterprise Risk Management*. Nell'ambito di tale *assessment*, a partire dagli esiti del precedente esercizio, ciascuna area è chiamata a verificare la sussistenza dei processi già elencati, i relativi rischi e controlli in essere, nonché ad integrare il framework complessivo con eventuali nuovi processi, rischi e controlli.

Alla redazione del piano partecipano la funzione incaricata dei controlli interni di Gruppo e il dipartimento General Counsel Italy, previa condivisione con il rappresentante legale della Succursale.

Una volta validato da Casa Madre, il piano viene formalizzato e condiviso con l'intera Sede Secondaria, informando ogni *manager* dei controlli che verranno attuati sulla propria area di competenza e del contributo attesa dal suo ufficio.

Il piano annuale si traduce in una serie di attività a differente scadenza temporale (mensile, trimestrale, annuale).

I controlli di secondo livello, in particolare, mirano alla verifica della conformità alla normativa e dell'adeguatezza dei processi, selezionati appunto in fase di redazione di pianificazione annuale. Tali controlli portano all'emissione di una

serie di raccomandazioni della funzione incaricata dei controlli interni all'ufficio oggetto del controllo: raccomandazioni da implementare necessariamente entro la scadenza definita. L'attività dei controlli di secondo livello, quindi, non si esaurisce nella nota finale del controllo ma prevede un'attività continua e costante di monitoraggio dell'implementazione e corretto mantenimento delle azioni correttive necessarie a valle delle raccomandazioni.

La Sede Secondaria riporta alla Casa Madre i risultati delle attività di controllo condotte e le principali evidenze ed azioni correttive che ne sono conseguite in una video-conferenza mensile alla quale partecipano almeno il responsabile della funzione di conformità della Succursale italiana (General Counsel Italy) e i referenti di Casa madre per le attività di controllo.

La società incaricata dei controlli di terzo livello, infine, svolge attività di *audit* secondo un piano pluriennale approvato dalla Casa Madre, con reportistica periodica e indicazione delle eventuali azioni correttive da adottare.

2.5 Il processo di redazione e implementazione del Modello

L'implementazione del Modello per la Sede Secondaria ha preso l'avvio da un'attenta analisi degli strumenti organizzativi, di gestione e controllo della stessa ed ha tenuto conto delle indicazioni fornite in materia, ad oggi, dalle autorità giudiziarie, unitamente a quelle espresse dalla dottrina e dalle principali associazioni di categoria (AIBE, ABI e Confindustria).
Il processo di realizzazione del Modello si è sviluppato in diverse fasi, basate sul rispetto dei principi di tracciabilità e verificabilità delle attività svolte.
Il punto di partenza è stato l'individuazione della mappa delle c.d. "**attività a rischio**" ovvero delle attività svolte nel cui ambito possono essere commessi i Reati secondo quanto espressamente previsto dall'art. 6, c. 2, lett. a) del Decreto.
Si è quindi provveduto alla valutazione del sistema di controllo interno già esistente a presidio dei rischi individuati e all'adozione di specifici Protocolli, finalizzati a governare i profili di rischio enucleati a seguito dell'attività di mappatura delle attività svolte, secondo quanto richiesto dall'art. 6 c. 2 lett. b) del Decreto.

In conformità a quanto richiesto dall'art. 6 c. 2 lett. d) e lett. e) del Decreto, si è provveduto quindi a:

- definire le caratteristiche, i ruoli e i compiti dell'Organismo di Vigilanza (così come riportato nel successivo par. 4), espressamente preposto al presidio dell'effettiva applicazione del Modello ed alla sua costante verifica in termini di adeguatezza ed efficacia;
- definire le modalità di diffusione del Modello e di relativa formazione del personale (così come indicato nel successivo par. 5);
- delineare un apparato sanzionatorio (riportato nel successivo par.6) per tutte le violazioni del Modello.

2.5.1 Risk Assessment

Il Modello della Sede Secondaria si basa sulla individuazione della mappa delle

attività a rischio, ovvero delle attività nel cui ambito possono essere commessi i Reati, secondo quanto espressamente previsto dall'art. 6, c. 2, lett. a) del Decreto.
La mappatura delle attività a rischio è stata realizzata tenendo conto della storia della Sede Secondaria, e della documentazione ufficiale rilevante e disponibile presso la Sede Secondaria stessa, al fine di meglio comprendere i processi e le attività svolte ed individuare le attività aziendali da analizzare. La mappatura è stata realizzata attraverso un processo di Risk Assessment basato sull'analisi dei processi e delle attività svolte da: (i) le funzioni della Sede Secondaria; (ii) società esterne a cui sono affidate attività in outsourcing da parte della Sede Secondaria sulla base di appositi contratti. In particolare, oltre al CEO Italy, sono state coinvolte ed oggetto di mappatura ai sensi del Decreto le seguenti Unità Organizzative:

- Partnership e Commerciale
- Corporate Operations
- People & Service
- Legal, Compliance & Internal Control
- Finance & Accounting
- Marketing

La metodologia utilizzata ha previsto il coinvolgimento di un gruppo di lavoro composto da professionisti esterni - con competenze in tema di *compliance* 231 – e risorse interne del Gruppo. Sono stati svolti colloqui con i referenti delle citate unità organizzative in quanto soggetti dotati di una conoscenza approfondita dei processi aziendali e dei meccanismi di controllo esistenti, al fine di costruire un Modello il più possibile aderente agli specifici ambiti operativi e alla struttura organizzativa della Società, che faccia riferimento a Reati il cui rischio di realizzazione sia realisticamente prevedibile.
I colloqui sono stati condotti con l'obiettivo di individuare i processi e le attività potenzialmente a rischio di commissione dei Reati, nonché i presidi già esistenti atti a mitigare i predetti rischi. Gli stessi sono serviti inoltre ad avviare il processo di sensibilizzazione rispetto alle previsioni di cui al Decreto e all'importanza del rispetto delle regole interne adottate da Younited S.A. per la prevenzione dei reati.

Sono state, pertanto, identificate le aree a rischio di commissione dei Reati e quelle strumentali, per tali intendendosi, rispettivamente, le aree di attività il cui svolgimento può dare direttamente adito alla commissione di una delle fattispecie di Reato e le aree in cui, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione di tali Reati.

I risultati di tale attività sono stati formalizzati attraverso la redazione della matrice dei rischi, condivisa con gli intervistati, che evidenzia: i profili di rischio – ossia l'indicazione dei potenziali Reati, la relativa econometria, i relativi mitiganti in essere (i presidi di controllo atti a prevenire la commissione degli stessi) sia descritti sia valutati econometricamente, i mitiganti pianificati da implementare, i risk owner, i relativi audit previsti.

Con riferimento ai mitiganti (presidi organizzativi), di controllo e comportamento

esistenti rispetto alle specifiche fattispecie di Reato, è stata condotta una valutazione econometrica della loro idoneità a mitigare i rischi individuati evidenziando, se ritenuto opportuno, i mitiganti mancanti da implementare.
In particolare, l'analisi è stata condotta con l'obiettivo di verificare:

- l'esistenza di regole comportamentali di carattere generale a presidio delle attività svolte;
- l'esistenza e l'adeguatezza di procedure che regolino lo svolgimento delle attività nel rispetto dei principi di controllo;
- il rispetto e l'attuazione concreta del generale principio di separazione dei compiti;
- l'esistenza di livelli autorizzativi a garanzia di un adeguato controllo del processo decisionale;
- l'esistenza di specifiche attività di controllo e di monitoraggio sulle attività sensibili;
- l'individuazione del rischio residuo ottenuto dal rischio inerente mitigata dai mitiganti

È importante evidenziare che la mappa delle attività a rischio così prodotta fotografa la situazione esistente alla data di redazione del presente Modello. L'evolversi delle attività aziendali e/o della normativa di riferimento richiederà il necessario aggiornamento della mappatura e anche lo svolgimento delle audit periodiche utilizzando la matrice dei rischi, al fine di ricomprendere gli eventuali rischi associabili alle nuove attività.
La documentazione predisposta nell'ambito delle attività di Risk Assessment sopra descritte al fine della formalizzazione delle analisi e delle valutazioni condotte è disponibile presso l'Archivio dell'OdV.

2.5.2 Risultanze delle attività di *Risk Assessment*

Le attività di *Risk Assessment* condotte hanno consentito di identificare i profili di rischio maggiormente rilevanti in ragione della specifica operatività della Sede Secondaria.

In particolare, sono stati identificati i profili di rischio inerenti alle seguenti fattispecie di reato, i quali sono visibili nella matrice dei rischi in ordine decrescente di rischiosità residua:

- Reati contro la Pubblica Amministrazione e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (artt. 24, 25 e 25 decies D. Lgs. 231/2001);
- Reati Societari (art. 25 ter D. Lgs. 231/2001);
- Reati con finalità di terrorismo o di eversione dell'ordine democratico, reati di criminalità organizzata e reati transnazionali (artt. 25 quater, 24 ter, 25 quinquies, 25 quaterdecies e L. n. 146/2006);
- Reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies D.Lgs. 231/01);
- Reati di ricettazione, riciclaggio, impiego di denaro beni o utilità di provenienza illecita nonché autoriciclaggio e Delitti in materia di strumenti di pagamento

diversi dai contanti (art. 25 octies e art. 25- octies.1 D. Lgs. 231/2001);
- Reati e illeciti amministrativi riconducibili ad abusi di mercato (art. 25 sexies D. Lgs. 231/2001);
- Reati in tema di salute e sicurezza sul lavoro (art. 25 septies D. Lgs. 231/2001);
- Delitti informatici (art. 24 bis D. Lgs. 231/2001);
- Reati contro l'industria e del commercio e in materia di violazione del diritto d'autore (artt. 25 bis.1, e 25 novies D. Lgs. 231/2001);
- Reati tributari (art. 25 quinquiesdecies D. Lgs. 231/2001).

Relativamente ai restanti reati del Decreto non sopra riportati, si è ritenuto che la specifica attività svolta dalla Sede Secondaria non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa. Si è pertanto considerato esaustivo il richiamo ai principi contenuti sia nel presente Modello che nel Codice Etico, ove si vincolano gli esponenti aziendali, i dipendenti ed i partner commerciali al rispetto dei valori di solidarietà, tutela della personalità individuale, correttezza, moralità e rispetto delle leggi.

2.5.3 Stesura del Modello di Organizzazione, Gestione e Controllo

Le attività di *risk assessment* precedentemente descritte e le relative risultanze sono state oggetto di condivisione con la Sede Secondaria.

A detta fase di analisi, diagnosi e progettazione, è seguita dunque la fase di realizzazione, che ha condotto alla stesura del presente Modello e alla definizione degli elementi che lo compongono.

In particolare, in conformità a quanto prescritto dall'art. 6 c. 2 lett. b) del Decreto, la Sede Secondaria, in aggiunta ai principi contenuti nel Codice Etico e nel corpus delle policy e procedure di Casa Madre già esistenti, ha provveduto a fornire ai Destinatari (cfr. *infra*) indicazioni in ordine alle condotte da tenere e a quelle da evitare, affinché non vengano poste in essere azioni idonee a realizzare fattispecie di reato e, in modo particolare, gli illeciti inclusi nell'elenco del Decreto, formalizzando a tal fine specifici Protocolli riportati nelle Parti Speciali del Modello.

2.5.4 Il sistema Whistleblowing e la tutela degli autori delle relative segnalazioni

La Legge n. 179/2017 ("Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato") aveva previsto l'obbligo di inserire, all'interno del Modello di Organizzazione, Gestione e Controllo, un sistema di segnalazione (whistleblowing) idoneo a consentire a dipendenti e collaboratori della Società di segnalare, in via riservata, violazioni o irregolarità delle quali fossero venuti a conoscenza in ragione delle funzioni svolte.
Successivamente, il Decreto Legislativo 10 marzo 2023, n. 24 ("Decreto

Whistleblowing"), che ha attuato la Direttiva (UE) 2019/1937, ha riordinato e in parte abrogato la normativa previgente, introducendo un quadro normativo organico e uniforme in materia di tutela dei segnalanti, applicabile sia al settore pubblico che a quello privato.
In particolare, la nuova formulazione dell'art. 6, comma 2-bis, del D.Lgs. 231/2001, così come modificato dal Decreto Whistleblowing, stabilisce che il Modello 231 debba:

- prevedere canali di segnalazione interna conformi ai requisiti normativi;
- garantire il divieto di atti ritorsivi o discriminatori nei confronti del segnalante;
- definire un sistema disciplinare idoneo a sanzionare eventuali violazioni delle misure a tutela del whistleblower.

In conformità a tale quadro normativo e nel rispetto dei principi contenuti nella Policy Whistleblowing di Gruppo, la Società ha adottato una specifica Procedura Whistleblowing che disciplina le modalità operative di gestione delle segnalazioni, assicurando:

- la tutela della riservatezza dell'identità del segnalante, del segnalato e dei soggetti eventualmente menzionati;
- la tracciabilità, integrità e conservazione della segnalazione;
- l'imparzialità e autonomia del soggetto gestore della segnalazione;
- la possibilità di effettuare segnalazioni anche in forma anonima, purché circostanziate.

La Procedura Whistleblowing si applica a tutti i soggetti che intrattengono un rapporto lavorativo o professionale con la Società, ed è parte integrante del sistema dei controlli previsto dal Modello 231.

Canali di segnalazione

La segnalazione interna consiste nell'invio di informazioni, come sopra definite, alle persone incaricate di raccogliere ed elaborare le segnalazioni ricorrendo ai seguenti canali di comunicazione: Scritta: mediante invio della segnalazione all'indirizzo e-mail **lanceurdalerte@younited-credit.fr**. L'accesso a tale indirizzo è limitato alle persone incaricate della raccolta e del trattamento delle segnalazioni (RCCI e Financial Director alla data dell'ultima pubblicazione).

La Succursale, in ottemperanza al D.lgs 24/2023, delle Line Guida emanate dall'ANAC in data 12/07/2023 in materia di whistleblowing, si dotata altresì di un canale di segnalazione interna costituito da una piattaforma informatica (*Whistleblowing software*) che garantisce la riservatezza dell'identità della persona segnalante, del segnalato e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. La piattaforma è separata dai sistemi informatici della Società poiché ospitata da un server indipendente ed è accessibile dalla sezione dedicata al "Whistleblowing" presente sul sito internet della Società e raggiungibile al seguente indirizzo:
https://whistleblowersoftware.com/secure/younitedwhistleblowingreports.
Nella medesima sezione sono disponibili la presente procedura, l'informativa sul trattamento dei dati personali e le istruzioni operative necessarie per trasmettere la segnalazione, ulteriormente dettagliate all'interno della piattaforma.

È possibile eseguire segnalazioni di potenziali e/o attuali illeciti lesivi del diritto

dell'unione Europea o delle disposizioni di cui al D.lgs. 231/2001, anche facendo ricorso alla piattaforma online resa disponibile dall'Autorità Nazionale Anticorruzione (ANAC).

3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

3.1. Finalità e struttura del Modello

L'adozione del Modello è tesa alla creazione di un sistema di prescrizioni e strumenti organizzativi avente l'obiettivo di: a) garantire che l'attività della Sede Secondaria sia svolta nel pieno rispetto del Decreto e b) prevenire e sanzionare eventuali tentativi di porre in essere comportamenti che determinino un rischio di commissione di un Reato.

Pertanto, il Modello si propone come finalità quelle di:

- valorizzare i presidi già in essere, atti a scongiurare le condotte illecite rilevanti ai sensi del Decreto incorporando anche strumenti del sistema di Corporate Governance di Younited S.A. e, laddove necessario, potenziare il sistema di controllo interno al fine di garantirne la piena conformità ai requisiti previsti dalla normativa italiana in materia di responsabilità degli enti e dotarsi di un sistema strutturato ed organico di prevenzione e controllo finalizzato alla mitigazione del rischio di commissione dei reati connessi all'attività aziendale;
- rendere noto a tutto il personale della Sede Secondaria che opera in Italia, l'oggetto ed il perimetro della richiamata normativa;
- determinare, in tutti coloro che operano in Italia in nome e per conto della Sede Secondaria nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ai sensi del Decreto, in un illecito passibile di sanzioni sia a carico dell'autore della violazione (sul piano civilistico, disciplinare e, in taluni casi, penale) sia a carico della Sede Secondaria (responsabilità amministrativa ai sensi del Decreto);
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse della Sede Secondaria che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni disciplinari oppure la risoluzione del rapporto contrattuale;
- ribadire che la Sede Secondaria non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la Younited si trovasse nella condizione di poterne probabilmente trarre vantaggio) sono contrari ai principi etici sostenuti dalla Younited S.A.;
- censurare fattivamente i comportamenti posti in essere in violazione del Modello attraverso l'irrogazione di sanzioni disciplinari e/o contrattuali.

Il Modello predisposto dalla Sede Secondaria si fonda, pertanto, su un sistema strutturato ed organico di protocolli, nonché di attività di controllo che nella sostanza:

- individuano le aree/i processi di possibile rischio nell'attività aziendale vale a

dire quelle attività nel cui ambito si ritiene più alta la possibilità che possano essere commessi i Reati;

- definiscono un sistema normativo interno, finalizzato alla prevenzione dei Reati, nel quale sono tra l'altro ricompresi:
  - un Codice Etico di Gruppo, che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali;
  - un sistema di deleghe, poteri e di procure per la firma di documenti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
  - procedure formalizzate, tese a disciplinare le procedure operative e le modalità controllo nei Processi a Rischio;
- trovano il proprio presupposto in una struttura organizzativa coerente con le attività aziendali, volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti della struttura organizzativa auspicati siano effettivamente realizzati, attraverso:
  - un organigramma formalmente definito, chiaro ed adeguato all'attività da svolgere;
  - una chiara definizione delle funzioni e delle responsabilità attribuite a ciascuna unità organizzativa;
  - un sistema di deleghe di funzioni interne e di procure a rappresentare la Sede Secondaria verso l'esterno che assicuri una chiara e coerente segregazione delle funzioni;
- individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- attribuiscono all'Organismo di Vigilanza della Sede Secondaria il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporne l'aggiornamento.
- prevedono un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello, applicabile tanto ai soggetti apicali quanto ai soggetti sottoposti all'altrui direzione o vigilanza, in coerenza con le disposizioni normative e contrattuali vigenti;
- definiscono un sistema di flussi informativi e obblighi di reporting nei confronti dell'Organismo di Vigilanza, da parte delle diverse funzioni aziendali, finalizzato a consentire un efficace controllo sull'attuazione del Modello e sull'emersione di eventuali criticità;
- stabiliscono le modalità di formazione e sensibilizzazione del personale in relazione ai contenuti del Modello, al Codice Etico, e alle procedure aziendali, al fine di assicurare una piena consapevolezza dei rischi e dei comportamenti richiesti;
- disciplinano le modalità di aggiornamento e revisione del Modello, prevedendo meccanismi volti ad adeguarlo in caso di modifiche normative, organizzative, operative o a seguito di significative violazioni accertate;
- si integrano con i presìdi già esistenti in materia di salute e sicurezza sul lavoro, privacy, anticorruzione e antiriciclaggio, al fine di garantire un approccio coordinato e sinergico alla compliance aziendale.

3.2. Natura del Modello e rapporti con il Codice Etico

Le prescrizioni contenute nel presente Modello integrano con quelle del Codice Etico del Gruppo, e si fondano sui medesimi principi di quest'ultimo.

Al riguardo, si evidenzia, altresì, che:

- il Codice Etico rappresenta uno strumento adottato in via autonoma ed è suscettibile di applicazione sul piano generale da parte della Sede Secondaria allo scopo di esprimere i principi di "deontologia aziendale" che le stesse riconoscono come propri e cui tutti i Destinatari devono attenersi;
- il Modello risponde invece alle specifiche esigenze previste dal Decreto, ed è finalizzato a prevenire la commissione di particolari tipologie di reati che, ove evidentemente commessi nell'interesse o a vantaggio della Sede Secondaria, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo.

3.3. Destinatari del Modello

Le prescrizioni del Modello sono indirizzate a tutti coloro che operano nella Sede Secondaria italiana di Younited S.A. e in particolare a quanti si trovino a svolgere le attività identificate a rischio, e precisamente ai seguenti soggetti:

- Organi Dirigenti della Sede Secondaria,
- soggetti apicali ovvero coloro che rivestono anche di fatto funzioni di rappresentanza, di amministrazione o di direzione della Sede Secondaria;
- tutti coloro che operano su operazioni cross border in Italia ed intrattengono con la Sede Secondaria un rapporto di lavoro subordinato (dipendenti), ivi compresi i dipendenti di Younited S.A. distaccati presso altre sedi e coloro che collaborano con la Sede Secondaria in forza di un rapporto di lavoro parasubordinato (fra questi: i lavoratori con contratto a progetto o a termine e gli stagisti);
- tutti coloro che intrattengono con la Sede Secondaria un rapporto di lavoro subordinato (dipendenti), ivi compresi i dipendenti di altre società facenti capo a Younited S.A. distaccati presso la Sede Secondaria e coloro che collaborano con la Sede Secondaria in forza di un rapporto di lavoro parasubordinato (fra questi: i lavoratori con contratto a progetto o a termine e gli stagisti).
- Dipendenti di altre società della Younited S.A. che svolgono attività in outsourcing a favore della Sede Secondaria (*Shared Services*) ai sensi di un Service Level Agreement.

Quanto ai soggetti Terzi – non riconducibili alle categorie sopraelencate che pur tuttavia operano su mandato o per conto o nell'interesse della Sede Secondaria, quali collaboratori esterni, Consulenti, fornitori, partner e tutti coloro che abbiano rapporti contrattuali con la Sede Secondaria per lo svolgimento di qualsiasi prestazione lavorativa con riferimento ad operazioni di Investment Banking *cross border* in Italia, o connesse all'Italia o a strumenti finanziari quotati in Italia, gli stessi sono tenuti al rispetto delle prescrizioni dettate dal Decreto e dei principi etici e comportamentali adottati dalla Sede Secondaria attraverso il Codice Etico mediante la sottoscrizione di apposite clausole contrattuali, che consentano alla Sede Secondaria in caso di inadempimento, di recedere dai contratti stipulati o

di risolverli, richiedendo il risarcimento dei danni eventualmente subiti (ivi compresa l'eventuale applicazione di sanzioni ai sensi del Decreto).

I Destinatari del Modello sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Sede Secondaria.

La Sede Secondaria condanna qualsiasi comportamento difforme rispetto alla legge italiana ed alle previsioni del Modello, anche qualora il comportamento sia posto in essere nell'interesse della Younited ovvero con l'intenzione di arrecare ad esse un vantaggio.

3.4. Adozione, modifiche e integrazioni del Modello

Il Decreto prevede che sia l'organo dirigente ad adottare ed efficacemente attuare il Modello, rimettendo ad ogni ente il compito di individuare al proprio interno l'organo cui affidare tale compito.

Le linee guida dell'ABI individuano nel consiglio di amministrazione l'organo di vertice delle banche. Tuttavia, in virtù della circostanza che le attività in Italia vengono svolte da succursali di una banca estera e alla luce della struttura organizzativa della Sede Secondaria, si è ritenuto di affidare il compito di adottare il Modello agli Organi Dirigenti della Sede Secondaria stessa.

Si è ritenuto inoltre di affidare al CEO Italy della Sede Secondaria il compito di provvedere all'attuazione del Modello nella succursale stessa, mediante valutazione e approvazione delle azioni proposte dall'OdV, necessarie per l'implementazione degli elementi fondamentali dello stesso Modello.

L'efficace e concreta attuazione del Modello da parte di funzioni italiane ovvero di funzioni estere che operano in Italia è garantita dai responsabili delle medesime funzioni a vario titolo coinvolti nelle "attività a rischio".

Fra le modifiche di carattere sostanziale rientrano, a titolo esemplificativo e non esaustivo:

- inserimento nel presente documento di ulteriori Parti Speciali;
- aggiornamento di alcune parti del presente documento;
- aggiornamento/modifica/integrazione dei principi di controllo e delle regole comportamentali.

4. ORGANISMO DI VIGILANZA

4.1. Identificazione dell'OdV

In base al Decreto, l'organismo di Vigilanza, che deve vigilare sul funzionamento e sull'osservanza del Modello, deve essere dotato di autonomi poteri di vigilanza e controllo.

In considerazione della peculiarità della Sede Secondaria, nonché della sua struttura organizzativa, caratterizzata dalla presenza di soggetti con incarichi operativi e/o direttamente coinvolti (anche in qualità di Process Owner) in potenziali Processi a Rischio, gli Organi Dirigenti della Sede Secondaria al fine di garantire i requisiti di autonomia, indipendenza, professionalità e continuità d'azione dell'OdV, potranno identificare i relativi componenti anche al di fuori dell'organico della Younited.

Pertanto, sulla base delle considerazioni formulate in precedenza, gli Organi Dirigenti della Sede Secondaria hanno individuato un Organismo di Vigilanza (OdV) a composizione collegiale, costituito da tre membri, di cui due esterni e uno interno all'organizzazione.
La Presidenza dell'OdV è affidata a un membro esterno, così da garantire adeguati requisiti di indipendenza, autonomia e professionalità.

L'OdV avrà comunque la facoltà di utilizzare altre risorse, interne (come Legal e Compliance, o l'Internal Control di Gruppo) o esterne, per lo svolgimento delle attività di controllo/verifica o dei propri compiti di natura più specificamente tecnica.

A garanzia dell'autonomia e in coerenza con quanto previsto dalle Linee Guida dell'ABI, nonché dalle Linee Guida di Confindustria, all'OdV è assegnato un budget annuo adeguato, proposto dall'Organismo stesso e approvato dall'Organo Dirigente.

L'attribuzione del ruolo di OdV a soggetti diversi da quelli qui identificati o la modifica delle funzioni assegnate all'OdV deve essere deliberata dagli Organi Dirigenti.

La composizione dell'OdV dovrà comunque essere tale da garantire la sua piena autonomia ed indipendenza nell'espletamento delle proprie funzioni, in ossequio ai dettami del Decreto nel rispetto del la continuità d'azione dello stesso.

4.2. Modalità di nomina e revoca

L'OdV è nominato dagli Organi Dirigenti. Con le medesime modalità, gli Organi Dirigenti provvedono anche alla nomina del Presidente dell'OdV.
Il perfezionamento della nomina dei membri dell'OdV si determina con la dichiarazione di accettazione da parte di questi ultimi formalizzata nel verbale della seduta degli Organi Dirigenti, oppure con la sottoscrizione per accettazione, da parte degli stessi, di una copia dell'estratto della relativa delibera.

Gli Organi Dirigenti valutano periodicamente l'adeguatezza dell'OdV in termini di struttura organizzativa e di poteri conferiti e possono, ove sussista una giusta causa, revocare l'incarico ad uno (o a tutti) i membri dell'OdV, come meglio specificato al paragrafo successivo.

Gli Organi Dirigenti provvedono, prima di ogni nuova nomina, a verificare la sussistenza dei requisiti espressamente richiesti dal Decreto per ciascun membro dell'OdV, nonché degli altri requisiti citati nel presente capitolo.

È responsabilità degli Organi Dirigenti provvedere alla tempestiva nomina del membro dell'OdV decaduto o revocato o il cui incarico sia comunque cessato.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza del Presidente, subentra a questi il membro più anziano (qualora l'OdV sia in composizione collegiale), il quale rimane in carica fino alla data in cui gli Organi Dirigenti abbiano deliberato la nomina del nuovo Presidente dell'OdV.

Durante l'eventuale periodo di *vacatio* per il verificarsi di uno egli eventi sopra delineati, in caso di OdV in composizione collegiale, i restanti membri dell'Organismo di Vigilanza restano in carica con l'onere di richiedere agli Organi Dirigenti di procedere tempestivamente alla nomina del membro mancante.

I membri dell'OdV potranno dimettersi dalla carica in qualsiasi momento, previa comunicazione da presentarsi per iscritto agli Organi Dirigenti, trasmessa in copia conoscenza agli altri componenti.

4.3. Cause di ineleggibilità e motivi di revoca

La nomina dei componenti dell'OdV è condizionata al possesso, da parte degli stessi, dei requisiti soggettivi di onorabilità, integrità, rispettabilità e professionalità e indipendenza, nonché all'assenza di cause di incompatibilità con la nomina stessa quali quelle descritte di seguito.

In primis, i componenti dell'Organismo di Vigilanza, dal momento della nomina e per tutta la durata della carica, non dovranno:

- trovarsi in una posizione di conflitto di interessi, anche potenziale, con la Sede Secondaria, tale da poter probabilmente pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'OdV;
- svolgere funzioni di tipo esecutivo direttamente connesse al business all'interno di, o delegate da, gli Organi Dirigenti;
- svolgere all'interno della Sede Secondaria funzioni di tipo esecutivo direttamente connesse al business;
- aver avuto un rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale membro dell'OdV ovvero all'instaurazione del rapporto di consulenza/collaborazione con lo stesso Organismo.

Inoltre, la Sede Secondaria ha stabilito che i componenti dell'OdV devono essere nominati tra soggetti in possesso di adeguata esperienza in materia giuridica e di controllo e gestione dei rischi aziendali, e non devono:

- trovarsi in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art.

2382 del codice civile;

- essere stati sottoposti a misure di prevenzione ai sensi della legge 27 dicembre 1956, n. 1423 o della legge 31 maggio 1965, n. 575 e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- aver riportato sentenza di condanna o patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione,
  - o per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267 (legge fallimentare);
  - o per uno dei delitti previsti dal titolo XI del Libro V del codice civile (società e consorzi);
  - per un delitto non colposo, per un tempo non inferiore a un anno;
  - per un delitto contro la Pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica ovvero per un delitto in materia tributaria;
  - per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
  - per uno dei reati previsti dal titolo XI del libro V del codice civile così come riformulato del d.lgs.61/02 (Disciplina degli illeciti penali e amministrativi riguardanti le società commerciali);
  - per un reato che importi e abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
  - per una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni (Disposizioni contro la mafia);
  - per le sanzioni amministrative accessorie previste dall'art. 187- quater del Testo Unico della Finanza).
- essere stati destinatari di un decreto che dispone il giudizio per uno dei Reati;
- aver svolto funzioni di amministratori esecutivi, nei tre esercizi precedenti alla nomina quali membri dell'Organismo di Vigilanza, in imprese:
  - sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;
  - operanti nel settore creditizio, finanziario, mobiliare e assicurativo sottoposte a procedure di amministrazione straordinaria.

Le regole sopra descritte si applicano anche in caso di nomina di un componente dell'OdV in sostituzione di altro membro dell'organismo stesso.

All'atto del conferimento dell'incarico, il soggetto designato a ricoprire la carica di membro dell'OdV deve rilasciare una dichiarazione nella quale attesta formalmente l'assenza dei motivi di incompatibilità ivi richiamati, la cui ricorrenza e permanenza verranno di volta in volta accertate dagli Organi Dirigenti.

I componenti dell'Organismo di Vigilanza decadono dalla carica nel momento in cui vengano a trovarsi successivamente alla loro nomina in una delle situazioni di ineleggibilità contemplate sopra. La decadenza dalla carica di componente dell'OdV opera automaticamente sin dal momento della sopravvenienza della

causa che l'ha prodotta, fermi restando gli ulteriori obblighi sotto descritti.
In caso di sopravvenuta causa di decadenza dalla carica, il membro dell'OdV interessato deve darne immediata comunicazione per iscritto agli Organi Dirigenti ed agli altri membri dell'Organismo di Vigilanza medesimo. Anche in assenza della suddetta comunicazione, ciascun membro dell'Organismo di Vigilanza che venga a conoscenza dell'esistenza di una causa di decadenza in capo ad un altro componente, deve darne tempestiva comunicazione per iscritto agli Organi Dirigenti per consentire al medesimo di adottare i necessari provvedimenti.

La revoca di uno o di tutti i membri dell'OdV e l'attribuzione di tali poteri ad altri soggetti, potrà avvenire soltanto per giusta causa, mediante un'apposita determinazione degli Organi Dirigenti**.**

A tale proposito, per "giusta causa" di revoca dell'incarico di membro dell'OdV potrà intendersi, a titolo meramente esemplificativo:

- la perdita dei requisiti soggettivi di onorabilità, integrità, rispettabilità, professionalità e indipendenza presenti in sede di nomina;
- il verificarsi di una causa di incompatibilità;
- la violazione dei doveri di riservatezza;
- la messa in atto di un comportamento gravemente colposo nell'assolvimento dei compiti connessi con l'incarico quale (a titolo meramente esemplificativo): l'omessa redazione e trasmissione agli Organi Dirigenti della relazione informativa periodica o del verbale riepilogativo annuale sull'attività svolta e l'omessa redazione del piano delle attività;
- l'"omessa o insufficiente vigilanza" da parte dell'OdV, secondo quanto previsto dall'art. 6, comma 1, lett. d), del Decreto;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'OdV.

In caso di revoca di tutti i membri dell'OdV, gli Organi Dirigenti hanno la facoltà di nominare un organismo ad interim.

4.4. Durata in carica dell'OdV

L'OdV dura in carica 3 anni, durante i quali i suoi membri potranno dimettersi dalla carica. Alla scadenza del loro mandato, i membri potranno essere rieletti.

4.5. Funzioni dell'OdV

L'OdV è completamente autonomo nell'esplicazione dei suoi compiti e le sue determinazioni sono insindacabili. In particolare, l'OdV deve:

- vigilare sull'osservanza del Modello da parte dei Destinatari;
- vigilare sull'efficienza e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;
- proporre e sollecitare l'aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali, normative, o di contesto esterno.

L'OdV deve inoltre operare:

- *ex-ante* (adoperandosi, ad esempio, per la formazione ed informazione del personale);
- continuativamente (attraverso l'attività di monitoraggio, di vigilanza sull'osservanza del Modello, l'attività di valutazione/analisi di eventuali necessità di aggiornamento del Modello da proporre agli Organi Dirigenti);
- *ex-post* (analizzando cause e/o circostanze che abbiano portato alla violazione delle prescrizioni del Modello o all'eventuale commissione di uno dei Reati).

Per un efficace svolgimento delle predette funzioni, all'OdV sono affidati i seguenti compiti e poteri:

- verificare periodicamente la mappa dei Processi a Rischio al fine di garantire l'adeguamento ai mutamenti dell'attività e/o della struttura aziendale;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al Modello;
- verificare periodicamente l'effettiva applicazione delle procedure aziendali di controllo nelle aree di attività a rischio e la loro efficacia;
- verificare l'adozione degli interventi a soluzione delle criticità in termini di sistemi di controllo interno, come rilevate in sede di risk assessment e/o di verifica;
- effettuare periodicamente verifiche su operazioni o atti specifici posti in essere nell'ambito dei Processi a Rischio;
- condurre indagini interne e svolgere attività ispettiva per accertare presunte violazioni delle prescrizioni del Modello;
- monitorare l'adeguatezza del sistema disciplinare previsto per i casi di violazione delle regole definite dal Modello;
- coordinarsi con le altre funzioni aziendali, nonché con gli altri organi di controllo, anche attraverso apposite riunioni, per il monitoraggio delle attività in relazione alle procedure stabilite dal Modello, o per l'individuazione di nuovi Processi a Rischio, nonché, in generale, per la valutazione dei diversi aspetti attinenti all'attuazione del Modello;
- coordinarsi e cooperare con i soggetti responsabili della tutela della salute e sicurezza dei lavoratori al fine di garantire che il sistema di controllo ai sensi del Decreto sia integrato con il sistema di controllo predisposto in conformità alle normative speciali per la sicurezza sui luoghi di lavoro;
- coordinarsi con i responsabili delle funzioni aziendali al fine di promuovere iniziative volte a sollecitare consapevolezza (anche con specifico riferimento all'organizzazione di corsi di formazione) e comprensione dei principi del Modello e per assicurare la predisposizione della documentazione organizzativa interna necessaria al funzionamento dello stesso, contenente

istruzioni, chiarimenti o aggiornamenti;
- effettuare verifiche periodiche sul contenuto e sulla qualità dei programmi di formazione.

A tal fine l'OdV avrà facoltà di:
- emanare disposizioni ed ordini di servizio intesi a regolare l'attività dell'OdV stesso;
- accedere ad ogni e qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'OdV ai sensi del Decreto;
- richiedere alle diverse strutture aziendali, anche di vertice, qualsiasi tipo di informazione ritenuta necessaria per l'assolvimento dei propri compiti, in modo che sia assicurata la tempestiva rilevazione di eventuali violazioni del Modello;
- effettuare verifiche periodiche sulla base di un proprio piano di attività nonché interventi "spot" non programmati nell'ambito di detto piano, ma comunque ritenuti necessari all'espletamento dei propri compiti.

Nello svolgimento dei propri compiti che gli competono, l'OdV avrà comunque la facoltà di ricorrere al supporto di collaboratori esterni, identificabili in soggetti appartenenti a qualsiasi funzione aziendale della Sede Secondaria che di volta in volta si rendesse utile coinvolgere per il perseguimento dei fini specificati e/o di consulenti terzi.

I collaboratori dell'OdV, su indicazione dell'OdV stesso, possono, anche individualmente, procedere alle attività di vigilanza ritenute opportune per il funzionamento e l'osservanza del Modello.

I soggetti appartenenti ad una funzione aziendale, nell'espletamento dell'incarico ad essi conferito in qualità di collaboratori dell'OdV, rispondono, gerarchicamente e funzionalmente, esclusivamente all'OdV.

L'OdV è dotato di un proprio Regolamento che ne assicura l'organizzazione e gli aspetti di funzionamento quali, ad esempio, la periodicità degli interventi ispettivi, le modalità di deliberazione, le modalità di convocazione e verbalizzazione delle proprie adunanze, la risoluzione dei conflitti d'interesse e le modalità di modifica/revisione del Regolamento stesso.
Inoltre, l'OdV potrà prevedere dei momenti formalizzati di incontro e confronto con soggetti interni e/o esterni alla Sede Secondaria, tra i quali, a titolo esemplificativo e non esaustivo:
- i soggetti chiave in materia di sistema di controllo interno della Sede Secondaria;

Obiettivo di detti incontri sarà principalmente il confronto ed il coordinamento con i soggetti coinvolti in prima linea nell'implementazione del sistema di controllo, ciascuno secondo l'area di propria pertinenza, al fine di consentire all'OdV di cogliere opportunità di miglioramento dei presidi in essere ai fini dell'efficacia del Modello. In tale ottica sarà cura dell'OdV verificare con i predetti soggetti l'efficacia dei flussi informativi nei suoi confronti, così come definiti al paragrafo "Obblighi di informazione verso l'Organismo di Vigilanza".

L'OdV provvederà a disciplinare le modalità operative e la periodicità di

organizzazione di detti incontri, individuando i soggetti di volta in volta coinvolti, nonché l'ordine del giorno degli stessi.

L'OdV, inoltre, provvederà a dotarsi di un Piano delle Attività che intende svolgere per adempiere ai compiti assegnatigli, da comunicare agli Organi Dirigenti.

Le attività di vigilanza svolte dall'OdV sono, di norma espletate tramite:
- audit cd. "ordinari", intendendosi per tali quelli programmati dall'Organismo;
- audit cd. "straordinari", intendendosi per tali quelli effettuati dall'OdV a seguito di una segnalazione o comunicazione ricevuta.

4.6. Obblighi di informazione verso l'Organismo di Vigilanza

Al fine di agevolare l'attività di vigilanza sull'effettività e sull'efficacia del Modello, l'OdV è destinatario di:

- *segnalazioni* relative a violazioni, presunte o effettive, del Modello (di seguito, "**Segnalazioni**");
- *segnalazioni di attività illecite* rilevanti ai sensi del D.Lgs. 231/2001 *da parte di un collaboratore*[7] *o un dipendente che ne sia venuto a conoscenza per ragioni di lavoro* (il cosiddetto **Whistleblowing**);
- *informazioni* utili e necessarie allo svolgimento dei compiti di vigilanza affidati all'OdV stesso (di seguito, "**Informazioni**").

Deve essere permesso all'OdV di accedere ad ogni tipo di informazione allo stesso necessaria al fine dello svolgimento della sua attività. Ne deriva di converso l'obbligo per l'OdV di mantenere confidenziali tutte le informazioni acquisite.

Nello specifico, **tutti i Destinatari** dovranno tempestivamente segnalare all'OdV casi di violazione, anche presunta, del Modello.

Tali Segnalazioni dovranno essere sufficientemente precise e circostanziate e riconducibili ad un definito evento o area; si precisa che tali Segnalazioni potranno riguardare qualsiasi ambito aziendale rilevante ai fini dell'applicazione del Decreto e del Modello vigente, ivi incluse le violazioni del Modello rilevanti ai fini della sicurezza e salute sul lavoro.

Si precisa altresì che è dovere anche dei Rappresentanti dei Lavoratori per la sicurezza, laddove tale funzione non sia svolta da un soggetto rientrante tra i Destinatari del Modello, di inviare tali Segnalazioni all'OdV.

Le comunicazioni e le segnalazioni possono essere inviate per iscritto a mezzo e-mail alla casella di posta **odv@younited-credit.it.**

Affinché l'OdV abbia accesso al maggior numero possibile di informazioni, la Sede Secondaria garantisce la tutela di qualunque segnalante contro ogni forma di ritorsione, discriminazione o penalizzazione, fatti salvi gli obblighi di legge e la tutela dei diritti della Sede Secondaria o delle persone accusate erroneamente

e/o in mala fede.
L'OdV valuterà le Segnalazioni ricevute con discrezionalità e responsabilità, provvedendo ad indagare, anche ascoltando l'autore della Segnalazione e/o il responsabile della presunta violazione, motivando per iscritto l'eventuale autonoma decisione di non procedere e dandone comunque comunicazione agli Organi Dirigenti nell'ambito del processo di reporting.

Al ricevimento di una Segnalazione riguardante una violazione, anche presunta, del Modello rilevante ai fini della sicurezza e salute sul lavoro, sarà onere dell'OdV verificare che il mittente abbia precedentemente o contestualmente informato anche il Datore di Lavoro e il Responsabile del Servizio di Prevenzione e Protezione.

Qualora il mittente della Segnalazione non vi abbia già provveduto, l'OdV provvederà ad informare tempestivamente il Datore di Lavoro e il Responsabile del Servizio di Prevenzione e Protezione.

In considerazione della potenziale rilevanza ai fini della determinazione di violazioni del Modello, l'Organismo di Vigilanza è informato circa le segnalazioni pervenute alla Younited alla seguente casella di posta elettronica: lanceurdalerte@younited-credit.fr.

In particolare, all'Organismo di Vigilanza è sottoposta mirata informativa, periodicamente (almeno annuale) ovvero ad evento se presenti elementi di rilevanza.

Con l'adozione del D.Lgs. 24/2023, recante attuazione della Direttiva (UE) 2019/1937 in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali, è stato introdotto nell'ordinamento italiano un quadro organico e vincolante in tema di whistleblowing.
In linea con tali previsioni, Younited ha adottato un sistema interno di segnalazione conforme ai requisiti normativi, volto a consentire ai dipendenti, ai collaboratori e ad altri soggetti qualificati la possibilità di segnalare in modo riservato e protetto violazioni di disposizioni normative nazionali o dell'Unione Europea, che ledano l'interesse pubblico o l'integrità dell'ente.

Per i dettagli operativi e le modalità di utilizzo dei canali, si rinvia alla procedura interna.

Flussi informativi ODV

L'Organismo di Vigilanza è destinatario, altresì, per conoscenza, con cadenza annuale, di apposita relazione sottoposta all'approvazione da parte degli Organi Aziendali. La predetta relazione ha ad oggetto il corretto funzionamento del dispositivo di allerta etico adottato e contiene le informazioni aggregate sulle attività svolte a seguito delle segnalazioni ricevute.
L'Organismo valuta le segnalazioni ricevute (direttamente o attraverso la casella di posta elettronica dalla Banca sopra indicata) e l'opportunità di azioni conseguenti, ascoltando, se necessario, l'autore della segnalazione e/o il

responsabile della presunta violazione. Di dette, eventuali audizioni va redatto specifico verbale. L'OdV è comunque tenuto a garantire la massima riservatezza circa l'identità dei segnalanti della cui identità sia venuto a conoscenza.
In particolare, i componenti dell'Organismo, nonché i soggetti dei quali l'Organismo stesso, a qualsiasi titolo, si avvale, sono tenuti a rispettare l'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni (fatte salve le attività di reporting periodico agli Organi).
I componenti dell'Organismo di Vigilanza assicurano la riservatezza delle informazioni di cui vengano in possesso, in particolare se relative a segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello.
I componenti dell'Organismo di Vigilanza si astengono dal ricevere e utilizzare informazioni riservate per scopi non conformi alle funzioni proprie dell'Organismo di Vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.
Le segnalazioni anonime non sono prese in considerazione, ciò non toglie tuttavia che, nel caso di segnalazioni anonime ma circostanziate (e, pertanto, contenenti tutti gli elementi oggettivi necessari alla successiva fase di verifica) l'Organismo di Vigilanza possa considerare eventuali ed ulteriori approfondimenti.

Oltre alle Segnalazioni sopra richiamate, in ogni caso, al fine di agevolare lo svolgimento dei propri compiti di vigilanza, l'OdV deve ottenere tempestivamente le seguenti Informazioni ritenute utili a tale scopo:

- le criticità, anomalie o atipicità riscontrate dalle funzioni aziendali nell'attuazione del Modello;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini nei confronti della Sede Secondaria e/o di altre società appartenenti al Gruppo per uno dei Reati;
- le comunicazioni interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di Reato;
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario per i Reati;
- le commissioni di inchiesta o le relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al Decreto;
- le notizie relative ai procedimenti disciplinari svolti con riferimento a violazioni del Modello e alle eventuali sanzioni irrogate (*ivi* compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le notizie relative a cambiamenti dell'assetto organizzativo;
- gli aggiornamenti del sistema delle deleghe e delle procure (ivi incluso il sistema poteri e deleghe in materia di sicurezza e salute sul lavoro);
- le notizie relative a cambiamenti organizzativi dei ruoli chiave in materia di sicurezza e salute sul luogo di lavoro (es: cambiamenti in merito a ruoli, compiti e soggetti delegati alla tutela dei lavoratori);
- modifiche al sistema normativo interno (incluse quelle in materia di sicurezza

e salute sul luogo di lavoro);
- copia del flusso informativo della Sede Secondaria.

Tali Informazioni devono essere fornite all'OdV a cura dei responsabili delle funzioni aziendali secondo le rispettive aree di competenza.

L'OdV può infine procedere alla raccolta delle informazioni ritenute necessarie all'esercizio dei suoi poteri di vigilanza anche attraverso appositi questionari che devono essere compilati dai Destinatari singolarmente individuati dall'OdV.

Inoltre, data la natura trasversale delle aree rilevanti in tema di reati in materia di sicurezza e salute sul lavoro, come meglio esplicitato nella relativa Parte Speciale (Capitolo 7) del Modello, le relative Informazioni dovranno essere trasmesse dai seguenti soggetti in quanto Destinatari del Modello ai sensi del par. 3.3, le seguenti figure organizzative, come definite dall'art. 2, D.Lgs. 9 aprile 2008, n. 81:
- il Datore di lavoro;
- il Delegato del Datore di lavoro (ove nominato);
- i Dirigenti;
- il Responsabile del Servizio di Prevenzione e Protezione;
- il Medico competente.

Infine, con riferimento alle aree rilevanti in tema di reati in materia di criminalità informatica, come meglio esplicitato nella relativa Parte Speciale (Capitolo 8) del Modello, le relative Informazioni dovranno essere trasmesse dal Responsabile IT.

Sarà infine cura dell'OdV definire e diffondere nei confronti dei Destinatari eventuali istruzioni, regole e meccanismi operativi specifici finalizzati a raccogliere ulteriori informazioni rilevanti relative alle attività svolte nelle aree/Processi a Rischio e ritenute particolarmente sensibili (quali, a tiolo puramente esemplificativo: l'avvio di nuovi *deal* con soggetti pubblici; l'assegnazione di incarichi a Consulenti; l'assegnazione di incarichi ad Appaltatori; l'avvio di contenziosi contrattuali; l'avvio di contenziosi con dipendenti o comunque attinenti l'area dei rapporti di lavoro; l'avvio di iniziative promozionali rivolte a soggetti pubblici; l'assunzione di nuovi dirigenti in capo alla Sede Secondaria; l'attività di sponsorizzazione, etc.). In particolare, tali informazioni ed elementi rilevanti potranno essere contenuti nella reportistica già attualmente prodotta a livello aziendale e/o di Gruppo, o, eventualmente, potranno essere raccolti attraverso altri strumenti/format/canali/modalità definiti dall'OdV stesso.

4.7. Reporting dell'OdV

L'OdV si riunisce su convocazione del Presidente almeno ogni tre mesi e, comunque, ogni volta che il Presidente lo ritenga opportuno ovvero che ne faccia richiesta scritta il membro interno con indicazione dell'ordine del giorno, nonché su convocazione dell'Organo Dirigente.

L'Organismo di Vigilanza riferisce per iscritto all'Organo Dirigente (come definito nel Modello 231), con cadenza semestrale, sull'attività compiuta nel periodo e sull'esito della stessa, fornendo se del caso una anticipazione sulle linee generali di intervento per il periodo successivo.
L'OdV riferisce in merito all'attuazione del Modello e alle eventuali criticità, direttamente agli Organi Dirigenti.

L'OdV, nei confronti dell'Organo Dirigente della Sede Secondaria ha la responsabilità di:

- comunicare, all'inizio di ciascun esercizio, il Piano delle Attività che intende svolgere per adempiere ai compiti assegnatigli;
- comunicare periodicamente, ed almeno semestralmente, lo stato di avanzamento del Piano delle attività, ed eventuali cambiamenti apportati allo stesso, motivandoli;
- segnalare tempestivamente qualsiasi violazione del Modello oppure condotte illegittime e/o illecite, di cui sia venuto a conoscenza per tramite Informazioni fornite dai Destinatari, che l'OdV ritenga fondate o che abbia accertato;
- redigere, almeno una volta l'anno, una relazione riepilogativa delle attività svolte nei precedenti dodici mesi e dei risultati delle stesse, degli elementi di criticità e delle eventuali violazioni del Modello, nonché delle proposte relative ai necessari aggiornamenti del Modello.

Gli Organi Dirigenti hanno la facoltà di convocare in qualsiasi momento l'OdV, il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti e di particolare gravità.

L'OdV potrà, inoltre, comunicare i risultati dei propri accertamenti ai responsabili delle funzioni qualora dalle verifiche svolte, scaturiscano carenze, comportamenti o azioni non in linea con il Modello. In tal caso, sarà necessario che l'OdV ottenga dai responsabili dei processi medesimi un piano delle azioni da intraprendere, con relativa tempistica, al fine di impedire il ripetersi di tali circostanze.

4.8. Conservazione delle informazioni

Tutte le Informazioni, Segnalazioni, rapporti e altri documenti raccolti e/o predisposti in applicazione del presente Modello sono conservati dall'OdV in un apposito archivio (informatico e/o cartaceo), gestito dall'organismo stesso, per un periodo di 10 anni.
L'accesso all'archivio è consentito esclusivamente ai membri del'OdV e/o ad eventuali collaboratori dello stesso debitamente incaricati.
Si precisa inoltre che anche la documentazione prodotta nell'ambito delle attività di predisposizione e aggiornamento del Modello (risk assessment, etc.) e raccolta in uno specifico archivio, è custodita a cura dell'OdV.

5. DIFFUSIONE DEL MODELLO

Ai fini dell'efficacia del Modello, è di primaria importanza la piena conoscenza delle regole di condotta ivi contenute sia da parte delle risorse già presenti nella Sede Secondaria alla data di approvazione del presente Modello, che di quelle che entreranno a farvi parte in futuro.

5.1. Comunicazione iniziale

Per garantire l'effettiva conoscenza, applicazione e comunicazione del Modello, viene data formalmente notizia dell'adozione dello stesso dall'Organo Dirigente a tutti i Destinatari.

In particolare, il Modello è reso disponibile a tutto il personale della Sede Secondaria Younited.

Ai soggetti terzi (fornitori, appaltatori, collaboratori, consulenti, professionisti, partner commerciali, ecc.) sono fornite apposite informative sui principi etici adottati dalla Sede Secondaria, in conformità al Modello ed al Codice Etico.

Per quanto riguarda i dipendenti neoassunti, il soggetto che riceve la comunicazione è tenuto a prendere visione del, ed impegnarsi ad aderire al, Modello. Si segue la medesima procedura ogniqualvolta si proceda ad un aggiornamento del Modello, che interessi una qualsiasi sua parte.

Per quanto attiene invece soggetti terzi qualunque contratto che comporti la costituzione di un rapporto commerciale o di qualunque forma di partnership con gli stessi deve esplicitamente contenere clausole di salvaguardia che attestino l'adozione di un sistema di controllo atto a prevenire il compimento dei Reati, che potrà anche risultare da documenti separati rispetto al contratto stesso, nonché il rispetto delle regole contenute nel Codice Etico del Gruppo.

5.2. Formazione del personale

La formazione del personale ai fini dell'attuazione del Modello è di competenza dell'Organo Dirigente che individua le risorse interne od esterne alla Sede Secondaria cui affidarne l'organizzazione.

Tali risorse procedono in coordinamento con l'OdV, che ne valuta l'efficacia in termini di pianificazione, contenuti, aggiornamento, tempistiche, modalità di identificazione dei partecipanti, nonché l'organizzazione delle sessioni di formazione.

La partecipazione alle suddette attività formative da parte dei soggetti individuati è ritenuta obbligatoria: conseguentemente, la mancata partecipazione a tali attività sarà sanzionata ai sensi del Sistema Disciplinare contenuto nel Modello.

La Sede Secondaria Younited ha previsto interventi di sensibilizzazione di tutto

il personale e momenti di formazione differenziati in relazione alla qualifica dei Destinatari e all'area di rischio in cui operano.

In particolare, per quanto attiene al personale della Sede Secondaria (sia che presti la propria attività lavorativa in forza di un contratto italiano, sia in forza di un contratto estero) e al personale di altre società italiane del Gruppo che prestano la propria attività per la Younited, è previsto un corso generale (in aula o con modalità e-learning) relativo alla illustrazione dei seguenti argomenti: i) quadro normativo di riferimento (Decreto e linee guida di categoria, etc.); ii) Modello adottato dalla Sede Secondaria; iii) Codice Etico; iv) casi aziendali di applicazione della normativa; v) presidi e protocolli introdotti a seguito dell'adozione del Modello.
I programmi di formazione in merito al Modello 231 avranno un contenuto minimo comune consistente nell'illustrazione dei principi del D.Lgs. n. 231/01, degli elementi costitutivi il Modello di Organizzazione Gestione e Controllo e a seconda dei destinatari della formazione e delle loro mansioni potranno contenere riferimenti a singole fattispecie di reati presupposto o ai comportamenti considerati sensibili in relazione al compimento dei reati sopra citati.
Ogni programma di formazione sarà modulato al fine di fornire ai suoi fruitori gli strumenti necessari e utili per comprendere e rispettare il Decreto in relazione all'ambito di operatività ed alle mansioni dei soggetti destinatari del programma stesso.

È inoltre previsto un corso di approfondimento in aula indirizzato all'Organo Dirigente e al personale che opera in "attività a rischio", in cui saranno illustrati le principali regole comportamentali ed i principi di controllo contenuti nelle Parti Speciali del Modello che il personale stesso dovrà seguire nell'espletamento delle proprie attività.
Per quanto concerne i neoassunti ovvero i soggetti che non potessero partecipare ai predetti corsi per comprovate ragioni, dovranno essere organizzati corsi specifici, eventualmente anche con modalità e-learning, previo accordo con il relativo responsabile di funzione.

Con riferimento al personale delle funzioni estere di Younited S.A. che opera sul territorio dello Stato italiano, si prevede un'attività di sensibilizzazione rispetto alla normativa italiana e sulla necessità di conformarsi alla stessa. In particolare, saranno erogati corsi di formazione che esplicitano la finalità del Decreto; le gravi conseguenze per la Società nell'ipotesi in cui venisse dichiarata la responsabilità della stessa ai sensi del Decreto o comunque derivanti dall'apertura di un procedimento penale a carico della medesima; le tipologie di illeciti ipoteticamente realizzabili.
I responsabili di dette funzioni estere provvederanno ad indicare alla Funzione Legal e Compliance di loro riferimento i soggetti che effettivamente svolgono attività *cross border* in Italia. A questi ultimi saranno altresì erogati i corsi innanzi descritti.

Della formazione effettuata dovrà essere tenuta puntuale registrazione.

Infine, la pianificazione della formazione deve prevedere sessioni periodiche che

garantiscano un costante programma di aggiornamento.

6. SISTEMA DISCIPLINARE

Il Decreto prevede che sia predisposto un "*sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*" sia per i soggetti in posizione apicale, che per i soggetti sottoposti ad altrui direzione. L'esistenza di un sistema di sanzioni applicabili in caso di mancato rispetto delle procedure interne previste dal Modello è, infatti, indispensabile per garantire l'effettività del Modello stesso.

L'applicazione delle sanzioni in questione deve restare del tutto indipendente dallo svolgimento e dall'esito di eventuali procedimenti penali avviati dall'autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto. Infatti, le regole di condotta imposte dal Modello sono assunte dalla Sede Secondaria in piena autonomia indipendentemente dal fatto che eventuali condotte possano costituire reato e che l'autorità giudiziaria intenda perseguire tale illecito.

In coerenza con il processo già adottato dalla Sede Secondaria, si prevede che le sanzioni da comminarsi a seguito di riscontrate violazioni al presente Modello siano proposte dall'OdV al soggetto titolare del potere disciplinare all'interno della Sede Secondaria.

6.1. Violazioni del Modello

Costituiscono violazioni del Modello di organizzazione, gestione e controllo della Sede Secondaria, a titolo esemplificativo e non esaustivo:

- comportamenti che integrino, direttamente o indirettamente, le fattispecie di reato contemplate nel Decreto;
- comportamenti che, sebbene non configurino uno dei Reati, siano inequivocabilmente strumentali alla relativa commissione;
- comportamenti non conformi alle procedure delineate dal Modello, volte a ridurre il rischio di commissione di uno dei Reati;
- comportamenti non conformi alle disposizioni previste nel Modello o richiamate dallo stesso e, in particolare dalle relative Parti Speciali;
- comportamenti non collaborativi nei confronti dell'OdV, ivi inclusi, a titolo esemplificativo e non esaustivo, il rifiuto di fornire le informazioni o la documentazione richiesta, il mancato rispetto delle direttive generali e specifiche rivolte dall'OdV al fine di ottenere le informazioni ritenute necessarie per l'assolvimento dei propri compiti, la mancata partecipazione senza giustificato motivo alle visite ispettive programmate dall'OdV, la mancata partecipazione agli incontri di formazione;
- violazione degli obblighi di informazione verso l'OdV.

Questa elencazione delle violazioni ha carattere esemplificativo e non si deve, dunque, ritenere completa, essendo possibili diverse ulteriori violazioni rispetto a quelle contenute nell'elenco.

L'Organismo di Vigilanza, accertata la sussistenza di una violazione del Modello, potrà segnalare la condotta rilevante al soggetto titolare del potere disciplinare della Sede Secondaria, richiedendo l'irrogazione della relativa sanzione, da determinarsi sulla base della gravità della violazione e della condotta complessiva dell'autore, sia antecedente (eventuali precedenti) sia successiva (collaborazione, ravvedimento, segnalazione spontanea).
Ai fini della valutazione della gravità della violazione saranno presi in considerazione, tra l'altro, i seguenti elementi:

- la sussistenza dell'elemento soggettivo (dolo, colpa grave, colpa lieve);
- l'eventuale recidiva;
- la prevedibilità e l'entità delle conseguenze dannose, attuali o potenziali, derivanti dalla violazione per la Sede Secondaria;
- la compromissione degli interessi tutelati dal Decreto, con particolare riferimento alla salute e sicurezza sul lavoro, alla tutela del patrimonio aziendale e alla compliance normativa;
- la posizione e il livello di responsabilità del soggetto autore della violazione;
- le modalità temporali, materiali e circostanziali della condotta;
- l'eventuale comportamento successivo, volto a mitigare le conseguenze della violazione o a collaborare con l'OdV.

L'irrogazione delle sanzioni dovrà in ogni caso avvenire nel rispetto delle previsioni normative e contrattuali applicabili, in coerenza con i principi di proporzionalità, tempestività e contraddittorio.

6.2. Misure nei confronti dei dipendenti

La violazione delle disposizioni comportamentali e procedurali contenute nel presente Modello da parte dei dipendenti della Sede Secondaria italiana – soggetti al Contratto Collettivo Nazionale di Lavoro per i dipendenti da aziende del Terziario, della Distribuzione e dei Servizi – Confcommercio, sottoscritto in data 30 luglio 2019 – costituisce illecito disciplinare.
Ai predetti lavoratori si applicano le sanzioni disciplinari previste dall'art. 22 del suddetto CCNL, irrogabili nel rispetto delle garanzie procedurali stabilite dall'art. 7 della Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), nonché di eventuali normative speciali applicabili. Le sanzioni disciplinari previste sono le seguenti:

a. biasimo inflitto verbalmente per le mancanze più lievi;
b. biasimo inflitto per iscritto in caso di recidiva;
c. multa in misura non eccedente l'importo corrispondente a mezza giornata di retribuzione;
d. sospensione dalla retribuzione e dal servizio per un periodo massimo di dieci giorni;
e. licenziamento per giusta causa, senza preavviso e con le ulteriori conseguenze di legge (c.d. licenziamento in tronco).

Ove la gravità della condotta lo giustifichi, ovvero qualora siano necessari specifici accertamenti istruttori, la Sede Secondaria potrà disporre – in via cautelativa – l'allontanamento temporaneo del lavoratore dal servizio per il tempo strettamente necessario, fermo restando il diritto di difesa del dipendente.

In relazione alla violazione delle disposizioni del Modello da parte dei dipendenti, si prevede quanto segue:

1. **Biasimo verbale o scritto**:

   È applicabile nei confronti del dipendente che violi le disposizioni del presente Modello, incluse le procedure interne e i protocolli relativi ai Processi a Rischio, quando la condotta non presenti profili tali da esporre concretamente la Sede Secondaria a responsabilità ai sensi del Decreto.

2. **Sospensione dalla retribuzione e dal servizio fino a 10 giorni**:

   Si applica nei confronti del dipendente che, violando le procedure previste dal presente Modello, cagioni un danno, anche potenziale, alla Sede Secondaria, ovvero ne metta a rischio l'integrità del patrimonio o l'affidabilità organizzativa, senza tuttavia configurare una condotta idonea a determinare l'applicazione di misure sanzionatorie ai sensi del Decreto.

3. **Licenziamento per giusta causa**:

   È applicabile nei confronti del dipendente che adotti una condotta:
   - chiaramente finalizzata alla commissione di un Reato rilevante ai sensi del Decreto;
   - oppure che, pur non integrando direttamente un Reato, sia idonea a determinare l'irrogazione di misure sanzionatorie nei confronti della Sede Secondaria ai sensi del D.Lgs. 231/2001, in ragione della gravità e dell'evidente violazione delle prescrizioni del Modello.

La funzione aziendale competente per l'irrogazione delle sanzioni disciplinari è tenuta a comunicare all'Organismo di Vigilanza (OdV) tutte le violazioni accertate del Modello, nonché i provvedimenti disciplinari adottati.

Art. 30 del D.Lgs. 81/2008
Il sistema disciplinare delineato nel presente Modello in materia di salute e sicurezza sui luoghi di lavoro si pone in stretta continuità con quanto previsto dall'art. 30 del D.Lgs. 9 aprile 2008, n. 81, il quale stabilisce che i modelli di organizzazione e gestione devono garantire un sistema aziendale idoneo ad assicurare l'adempimento di tutti gli obblighi giuridici in materia di prevenzione.
In particolare, l'art. 30 riconosce **efficacia esimente della responsabilità amministrativa dell'ente**, ai sensi del D.Lgs. 231/2001, qualora il modello sia adottato ed efficacemente attuato e sia dotato, tra l'altro, di:
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure previste;
- un sistema di controllo e verifica dell'attuazione del modello e del

mantenimento nel tempo delle condizioni di idoneità.

Con specifico riferimento alle violazioni delle disposizioni del presente Modello afferenti alla materia della salute e sicurezza sui luoghi di lavoro, si prevedono le seguenti misure disciplinari, graduabili in funzione della gravità della condotta posta in essere:

1. **Sospensione dalla retribuzione e dal servizio per un periodo massimo di dieci giorni**:

   Tale sanzione si applica al dipendente che, violando le procedure interne previste dal presente Modello in materia di salute e sicurezza, abbia tenuto una condotta connotata da negligenza, imprudenza o imperizia – ad esempio durante le attività di formazione, addestramento o esecuzione delle proprie mansioni – tale da determinare un **rilevante rischio differenziale**, inteso come incremento significativo del rischio di applicazione alla Sede Secondaria delle misure sanzionatorie previste dal Decreto.

2. **Licenziamento per giusta causa (senza preavviso)**:

   Si configura nei confronti del dipendente che, in violazione delle prescrizioni del presente Modello in materia di salute e sicurezza sui luoghi di lavoro, adotti una condotta tale da **esporre la Sede Secondaria a un rischio concreto e immediato di applicazione delle misure previste dal Decreto**, ovvero tale da generare un pericolo grave per la propria o altrui incolumità.

   A titolo meramente esemplificativo, rientrano in tale fattispecie comportamenti gravemente negligenti, imprudenti o imperiti, idonei a provocare incidenti, infortuni o danni a persone o cose, anche in assenza dell'effettiva verificazione dell'evento lesivo.

Le violazioni di regole comportamentali di cui al presente Modello da parte del personale di Younited S.A. che operi in Italia comporterà l'adozione dei provvedimenti disciplinari espressamente previsti in conformità alla legislazione locale: tali sanzioni sono altresì comminabili per ogni violazione delle normative locali, dei principi etici e delle policy della Società.

6.3. Violazioni del Modello da parte dei dirigenti e relative misure

Per quanto attiene alle violazioni di singole regole di cui al presente Modello, poste in essere dai dirigenti della Sede Secondaria, anche queste costituiscono illecito disciplinare.
Qualsiasi tipo di violazione delle regole contenute nel Modello autorizza l'OdV a richiedere alle funzioni aziendali competenti della Sede Secondaria l'irrogazione di una delle sanzioni di seguito elencate, sulla base della gravità della violazione commessa alla luce dei criteri indicati nel paragrafo 6 e del comportamento tenuto prima (e.g. eventuali precedenti violazioni commesse) e dopo il fatto (e.g. comunicazione all'OdV dell'avvenuta irregolarità) dall'autore della violazione.

I provvedimenti disciplinari irrogabili nei riguardi dei dirigenti della Sede Secondaria - nel rispetto delle procedure previste dall'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori), delle eventuali normative speciali applicabili, e del CCNL Dirigenti sono le seguenti:

a. censura scritta;
b. sospensione disciplinare;
c. licenziamento per giustificato motivo;
d. licenziamento per giusta causa.

In ogni caso, la funzione aziendale competente terrà sempre informato l'OdV in relazione alle sanzioni irrogate e/o alle violazioni accertate.
In particolare, con riferimento alle violazioni del Modello poste in essere dai dirigenti della Sede Secondaria, si prevede che:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nella **censura scritta** consistente nel richiamo all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Sede Secondaria;
- in caso di violazione non grave, ma reiterata, di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel provvedimento di **sospensione disciplinare**;
- in caso di grave violazione di una o più regole procedurali o comportamentali previste nel Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento di **licenziamento per giustificato motivo**;
- laddove la violazione di una o più regole procedurali o comportamentali previste nel Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il dirigente incorre nel provvedimento di **licenziamento per giusta causa**.

Inoltre, per i lavoratori della Sede Secondaria aventi qualifica di 'dirigente' costituisce grave violazione delle prescrizioni del Modello:

- l'inosservanza dell'obbligo di direzione o vigilanza sui lavoratori subordinati circa la corretta ed effettiva applicazione del Modello stesso.
- l'inosservanza dell'obbligo di direzione e vigilanza sugli altri lavoratori che, sebbene non legati alla Sede Secondaria da un vincolo di subordinazione (trattasi, ad esempio, di lavoratori autonomi, agenti, consulenti, collaboratori coordinati e continuativi ecc.), sono comunque soggetti alla direzione e vigilanza del 'Dirigente' ai sensi dell'art. 5 comma 1 lett. b) del Decreto, ferma restando la qualificazione giuridica del contratto con tali lavoratori.

Le violazioni di regole comportamentali di cui al presente Modello da parte del personale estero che operi in Italia comporterà l'adozione dei provvedimenti disciplinari espressamente previsti ai sensi della normativa locale: tali sanzioni sono comminabili per ogni violazione delle normative locali, dei principi etici e delle policy della Casa Madre.

6.4. Misure nei confronti dei lavoratori in regime di distacco da

altre società del Gruppo

Le violazioni commesse dai lavoratori che operano in regime di distacco (totale o parziale) da altre sedi di Younited S.A. presso la Sede Secondaria saranno sanzionate dalla sede distaccante attraverso l'adozione di un provvedimento ritenuto opportuno e compatibile con la vigente normativa e secondo le regole sanzionatorie interne della medesima sede distaccante. A tal fine la Sede Secondaria e la sede distaccante provvedono alla predisposizione, modifica e/o integrazione dei contratti (o di altri accordi e/o di qualsiasi atto di formalizzazione del distacco), prevedendo l'inserimento di opportune clausole all'interno degli stessi.

6.5. Misure nei confronti dei Consulenti, collaboratori, Appaltatori

Ogni violazione della parte generale del Modello e del Codice Etico posta in essere dai Consulenti/Partner, collaboratori esterni (ivi compresi i lavoratori somministrati e i lavoratori a progetto) e Appaltatori, nonché la commissione da parte degli stessi di uno dei Reati, potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di partnership, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento, qualora da tale comportamento derivino danni alla Sede Secondaria, come nel caso di applicazione da parte del giudice delle misure previste dal Decreto.
Se trattasi di soggetto straniero o operante all'estero, i contratti dovranno contenere l'obbligo di rispettare la normativa internazionale e locale di prevenzione dei rischi che possono determinare la responsabilità conseguente alla commissione di reati in capo alla Sede Secondaria.

6.6. Misure nei confronti dell'Organo Dirigente

La messa in atto di gravi inosservanze, di azioni o comportamenti non conformi alle prescrizioni e delle procedure previste o richiamate dal Modello da parte dell'Organo Dirigente è sanzionata con i provvedimenti disciplinari già previsti a seconda della gravità della violazione ed in considerazione della particolare natura del rapporto.
Rientrano tra le gravi inosservanze, a titolo esemplificativo e non esaustivo, l'omessa segnalazione all'Organismo di Vigilanza di qualsiasi violazione alle norme previste dal Modello di cui l'Organo Dirigente venisse a conoscenza, nonché il non aver saputo – per negligenza o imperizia - individuare e conseguentemente eliminare violazioni del Modello e, nei casi più gravi, perpetrazione di reati.

In particolare, in caso di violazioni da parte degli Organi Dirigenti della Sede Secondaria, l'OdV ne darà comunicazione immediata agli organi di controllo deputati a vigilare sull'attività della Sede stessa, per consentire l'adozione degli opportuni provvedimenti.

Misure relative alla violazione della normativa sulle segnalazioni

Ai sensi dell'art. 6, comma 2-*bis* del Decreto, il mancato rispetto della normativa relativa alle segnalazioni, è sanzionato dagli organi competenti in base alle regole interne della Società e del CCNL di riferimento nei seguenti casi:

(a) violazione dell'obbligo di riservatezza nei confronti dei soggetti coinvolti nella Segnalazione;

(b) commissione di condotte ritorsive e/o discriminatorie, dirette e indirette, nei confronti del soggetto che abbia effettuato le Segnalazioni e ai soggetti al medesimo equiparati;

(c) commissione di qualsiasi atto volto ad ostacolare, anche solo in modo tentato, la Segnalazione;

(d) non istituzione del canale di Segnalazione, o di procedure per la gestione delle medesime, o adozione di procedure non conformi a quanto previsto dal Decreto *Whistleblowing*;

(e) mancato svolgimento dell'attività di gestione della Segnalazione;

(f) effettuazione, con dolo o colpa grave, di Segnalazioni che si rivelino infondate.

PARTE SPECIALE

1.CARATTERISTICHE, STRUTTURA E OBIETTIVI DELLA PARTE SPECIALE

La presente Parte Speciale fornisce una breve descrizione dei Reati, focalizzandosi, in particolare, sui Reati che potrebbero essere commessi nell'ambito dell'attività svolta dalla Sede Secondaria.

Per ogni tipologia di Reato che si ritiene possa essere commesso da Younited sono stati identificati i Processi a Rischio, nell'ambito dei quali tali reati potrebbero configurarsi, nonché le regole di condotta finalizzate alla prevenzione di ciascuna tipologia di Reato.
Sulla base delle considerazioni svolte nella fase di Risk Assessment, i Reati potenzialmente configurabili in relazione alla realtà delle Branch sono stati suddivisi nelle seguenti tipologie:

- Reati contro la Pubblica Amministrazione e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (artt. 24, 25 e 25 decies D. Lgs. 231/2001);
- Reati Societari (art. 25 ter D. Lgs. 231/2001);
- Reati con finalità di terrorismo o di eversione dell'ordine democratico, reati di criminalità organizzata e reati transnazionali (artt. 25 quater, 24 ter, 25 quinquies, 25 quaterdecies e L. n. 146/2006)
- Reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies D.Lgs. 231/01)
- Reati di ricettazione, riciclaggio, impiego di denaro beni o utilità di provenienza illecita nonché autoriciclaggio e Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 octies e art. 25- *octies.*1 D. Lgs. 231/2001);
- Reati e illeciti amministrativi riconducibili ad abusi di mercato (art. 25 sexies D. Lgs. 231/2001);
- Reati in tema di salute e sicurezza sul lavoro (art. 25 septies D. Lgs. 231/2001);
- Delitti informatici (art. 24 bis D. Lgs. 231/2001);
- Reati contro l'industria e del commercio e in materia di violazione del diritto d'autore (artt. 25 bis.1 e 25 novies D. Lgs. 231/2001);
- Reati tributari (art. 25 quinquiesdecies D. Lgs. 231/2001).

Oltre alla identificazione di Processi a Rischio e dei relativi potenziali Reati, sono state altresì individuati, in relazione a ciascun Reato e ciascun processo, gli elementi specifici riconducibili alle componenti del sistema di organizzazione, gestione e controllo che costituiscono il Modello della Sede Secondaria (sistema di principi etici e regole di comportamento, sistema organizzativo, sistema autorizzativi, sistema di controllo).

Pertanto, obiettivo generale di questa parte del Modello è che tutti i Destinatari (dipendenti, soggetti con ruoli di vertice all'interno della Sede Secondaria, Consulenti, *Partner* e Appaltatori) adottino comportamenti conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi delle fattispecie di reato descritte nella Parte Speciale.

2. LE COMPONENTI DEL SISTEMA DI CONTROLLO PREVENTIVO

Le componenti (protocolli) del sistema di controllo preventivo che devono essere attuati a livello aziendale per garantire l'efficacia del Modello sono:

- principi etici finalizzati alla prevenzione dei Reati;
- sistema organizzativo sufficientemente formalizzato e chiaro;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali definite;
- procedure operative, manuali od informatiche, volte a regolamentare le attività a rischio nelle aree aziendali con gli opportuni punti di controllo;
- sistema di controllo di gestione in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità;
- sistema di comunicazione e formazione del personale avente ad oggetto tutti gli elementi del Modello, compreso il Codice Etico;
- sistema disciplinare adeguato a sanzionare la violazione delle norme del Codice Etico e delle altre disposizioni del Modello.

Fatte comunque salve le prescrizioni del presente Capitolo aventi caratteristiche comuni in relazione a tutte le fattispecie di Reato, si rinvia alle singole parti speciali per quanto concerne invece i protocolli aventi caratteristiche specifiche per ciascuna tipologia di Reati.
Con riferimento al Codice Etico, all'Organismo di Vigilanza, al sistema disciplinare ed al sistema di comunicazione e di formazione del personale, si rimanda a quanto previsto in precedenza nei Capitoli specificamente dedicati della Parte Generale del Modello.

2.1. Sistema organizzativo

Il sistema organizzativo della Sede Secondaria viene definito attraverso la predisposizione di un organigramma societario e l'emanazione di Deleghe di funzioni e disposizioni organizzative, che forniscono una chiara definizione delle funzioni e delle responsabilità attribuite a ciascuna unità organizzativa.

Con riferimento alla Sede Secondaria, la formalizzazione, l'aggiornamento e diffusione di detti documenti viene assicurata dall'area General Counsel Italy**,** previa approvazione da parte dell'Organo Dirigente.

2.2. Sistema autorizzativo

Il sistema autorizzativo, che consiste in un sistema coordinato e coerente rispetto alle Deleghe di poteri e procure della Sede Secondaria deve uniformarsi alle seguenti prescrizioni:

- le Deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- ciascuna Delega deve definire e descrivere in modo specifico ed inequivocabile i poteri gestionali del delegato ed il soggetto cui il delegato riporta gerarchicamente;
- i poteri gestionali assegnati con le Deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli;
- le Procure possono essere conferite esclusivamente a soggetti dotati di delega di poteri o di specifico incarico e devono prevedere l'estensione dei poteri di rappresentanza e, eventualmente, i limiti di spesa numerici;
- tutti coloro che intrattengono per conto della Sede Secondaria rapporti con la Pubblica Amministrazione, devono essere adeguatamente autorizzati;
- una procedura *ad hoc* deve disciplinare modalità e responsabilità per garantire un aggiornamento tempestivo delle Procure, stabilendo i casi in cui le Procure devono essere attribuite, modificate e revocate (assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui la Procura era stata conferita, dimissioni, licenziamento, ecc.).

2.3. Processo decisionale

Il processo decisionale afferente ai Processi a Rischio deve ispirarsi ai seguenti criteri:

- ogni decisione operativa nell'ambito dei Processi a Rischio come di seguito individuati deve risultare da un documento scritto;
- deve essere garantita la segregazione dei compiti, assicurando il coinvolgimento di più funzioni/soggetti nell'ambito del medesimo Processo a Rischio, nonché la segregazione funzionale delle attività operative e di

controllo;
- la ripartizione e attribuzione dei poteri autorizzativi e decisionali, nonché delle responsabilità delle strutture della Sede Secondaria, deve essere basata su principi di trasparenza, chiarezza e verificabilità delle operazioni, in conformità al sistema di poteri e deleghe adottato.

2.4. Controllo di gestione e flussi finanziari

L'art. 6, lett. c del Decreto esplicitamente statuisce che il Modello debba "*individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati*".
A tale scopo, il sistema di controllo di gestione adottato dalla Sede Secondaria è articolato nelle diverse fasi di elaborazione del Budget annuale, di analisi dei consuntivi periodici e di elaborazione delle previsioni a livello di locale.
Il sistema garantisce la:
- pluralità di soggetti coinvolti, in termini di congrua segregazione delle funzioni per l'elaborazione e la trasmissione delle informazioni;
- capacità di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità attraverso un adeguato e tempestivo sistema di flussi informativi e di reporting.

La gestione delle risorse finanziarie è definita sulla base di principi improntati ad una sostanziale segregazione delle funzioni, tale da garantire che tutti gli esborsi siano richiesti, effettuati e controllati da funzioni indipendenti o soggetti per quanto possibile distinti, ai quali, inoltre, non sono assegnate altre responsabilità tali da determinare potenziali conflitti di interesse.
Infine, la gestione della liquidità è ispirata a criteri di conservazione del patrimonio, con connesso divieto di effettuare operazioni finanziarie a rischio, ed eventuale doppia firma per impiego di liquidità per importi superiori a soglie predeterminate.

2.5. Programma di informazione e formazione

Con specifico riferimento alle attività realizzate nell'ambito dei Processi a Rischio, viene previsto e garantito un adeguato programma di informazione e formazione periodico e sistematico rivolto a dipendenti e collaboratori esterni coinvolti nelle stesse.

Il programma include la trattazione di tematiche di corporate governance e di divulgazione di meccanismi operativi e procedure organizzative aziendali rilevanti con riferimento alle materie riguardanti i Processi a Rischio.
Tali attività integrano e completano il percorso di informazione e formazione sul tema specifico delle attività poste in essere dalla Sede Secondaria al fine di garantire il rispetto del Decreto, previsto e disciplinato specificamente nei Capitoli a ciò dedicati della Parte Generale del Modello.

2.6. Sistemi informativi e applicativi informatici

Al fine di presidiare l'integrità dei dati e l'efficacia dei sistemi informativi e/o gli

applicativi informatici utilizzati per lo svolgimento di attività operative o di controllo nell'ambito dei Processi a Rischio, o a supporto delle stesse, è garantita la presenza e l'operatività di:

- sistemi di profilazione delle utenze in relazione all'accesso a moduli o ambienti;
- regole per il corretto utilizzo dei sistemi ed ausili informativi aziendali (supporti hardware e software);
- meccanismi automatizzati di controllo dell'accesso ai sistemi;
- meccanismi automatizzati di blocco o inibizione dell'accesso.

2.7. Archiviazione della documentazione

Le attività condotte nell'ambito dei Processi a Rischio dovranno essere adeguatamente formalizzate, con particolare riferimento alla documentazione predisposta nell'ambito della realizzazione delle stesse.

La documentazione sopra delineata, prodotta e/o disponibile su supporto cartaceo od elettronico, è archiviata in maniera ordinata e sistematica a cura delle funzioni coinvolte, o specificatamente individuate in procedure o istruzioni di lavoro di dettaglio.

Per la salvaguardia del patrimonio documentale ed informativo aziendale sono previste adeguate misure di sicurezza a presidio del rischio di perdita e/o alterazione della documentazione riferita ai Processi a Rischio o di accessi non autorizzati ai dati/documenti.

Con particolare riferimento alla documentazione in formato elettronico prodotta o archiviata su supporti informatici aziendali si rimanda inoltre a quanto definito al paragrafo precedente.

3. I REATI SOCIETARI (ivi comprese le fattispecie di corruzione tra privati)

3.1. Premessa

La presente Parte Speciale ha l'obiettivo di illustrare i criteri, i ruoli e le responsabilità, i principi di controllo e le regole di comportamento cui tutti i Destinatari, ivi compresi i Consulenti, il personale, i fornitori e i partner, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dagli articoli 25-*ter* del Decreto, nel rispetto dei principi di legalità, correttezza, oggettività, trasparenza, tracciabilità e riservatezza nell'esecuzione delle proprie attività, della normativa emanata dagli organismi di vigilanza e di tutte le leggi e le norme nazionali ed internazionali vigenti.
I reati societari considerati hanno ad oggetto differenti ambiti, tra i quali assumono particolare rilevanza la formazione del bilancio, le comunicazioni esterne, talune operazioni sul capitale, l'impedito controllo e l'ostacolo

all'esercizio delle funzioni di vigilanza, fattispecie accomunate dalla finalità di tutelare la trasparenza nei documenti contabili e nella gestione societaria e la corretta informazione ai soci, ai terzi ed al mercato in generale.

3.2. Le fattispecie di reato previste dall'art 25-*ter* del Decreto

Nell'ambito dei reati societari considerati dal Decreto, i reati che si ritiene che possano più facilmente trovare manifestazione nell'ambito delle attività svolte dalla Sede Secondaria sono i seguenti:

False comunicazioni sociali (art. 2621 c.c.) – Tale ipotesi di reato si realizza se gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci, i liquidatori della società, con l'intenzione di ingannare i soci o il pubblico e al fine di trarre ingiusto profitto, espongono nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ovvero omettono di fornire notizie la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del Gruppo di appartenenza, in modo concretamente idoneo a indurre in errore i destinatari delle suddette comunicazioni. Peraltro, la fattispecie si configura anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi;
Fatti di lieve entità (Art. 2621-*bis* c.c.) – La fattispecie, introdotta nell'ordinamento dalla L. 69/2015, si realizza qualora i fatti di cui al precedente articolo siano di lieve entità, sulla base di una valutazione giudiziale che tenga conto della natura e delle dimensioni della società, delle modalità o degli effetti della condotta, ovvero nel caso in cui siano commessi da società che non rientrano nei limiti definiti per l'applicabilità della disciplina del fallimento, ai sensi dell'art. 1, co. 2 del Regio Decreto n. 267 del 16 marzo 1942.
False comunicazioni sociali delle società quotate (art. 2622 c.c.) – Tale fattispecie di reato, introdotta dalla L. 69/2015, si configura qualora, in specifico riferimento a società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongano fatti materiali non rispondenti al vero ovvero omettano fatti materiali rilevanti la cui comunicazione sia imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore.
Tale fattispecie, analogamente a quella descritta dall'art. 2621, potrebbe essere commessa qualora, in concorso con un cliente, la Società predisponga documentazione ufficiale destinata al pubblico (ad esempio in relazione ad una specifica operazione) che sia tale da indurre in errore il pubblico circa la situazione economico-finanziaria del cliente stesso.
Impedito controllo (2625, 2° comma c.c.) – Tale reato si configura qualora, occultando documenti o con altri artifici, gli amministratori della Società impediscano o comunque ostacolino lo svolgimento delle attività di controllo

legalmente attribuite ai soci o agli altri organi societari, cagionando un danno ai soci.
Anche la suddetta fattispecie, analogamente alla precedente, potrebbe essere realizzata in concorso con il cliente, in relazione ad una specifica operazione;

Indebita Restituzione Dei Conferimenti (Art. 2626 C.C.) Il reato di indebita restituzione dei conferimenti riguarda la tutela dell'integrità del capitale sociale e si configura quando gli amministratori, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

Illegale Ripartizione Degli Utili E Delle Riserve (Art. 2627 C.C.) Tale reato si realizza quando gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite.

La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Illecite Operazioni Sulle Azioni O Quote Sociali O Della Società Controllante (Art. 2628 C.C.) Il reato di illecite operazioni sulle azioni o quote sociali o della società controllante prevede che gli amministratori i quali, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno. La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

Operazioni In Pregiudizio Dei Creditori (Art. 2629 C.C.) Tale ipotesi di reato consiste nel fatto che gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni, scissioni con altre società cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Formazione Fittizia Del Capitale (Art. 2632 C.C.) Tale reato prevede che gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni

in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

False O Omesse Dichiarazioni Per Il Rilascio Del Certificato Preliminare (Art. 54 D. Lgs. N. 19/2023) L'art. 54 del Decreto Legislativo n.19/2023, ha introdotto il nuovo reato di "False o omesse dichiarazioni per il rilascio del certificato preliminare".

La fattispecie punisce la condotta di chiunque al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'articolo 29, forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette informazioni rilevanti, è punito con la reclusione da sei mesi a tre anni.

Aggiotaggio (Art. 2637 c.c.) – Tale fattispecie ricorre qualora, ad esempio, il soggetto apicale della Società diffonda notizie false, ovvero si pongano in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (Art. 2638 c.c.) - Tale reato si realizza qualora nelle comunicazioni con le autorità di vigilanza previste ai sensi della normativa applicabile si espongano fatti materiali non corrispondenti al vero sulla situazione economica o finanziaria dei sottoposti alla vigilanza, ovvero si occultino con altri mezzi fraudolenti fatti che si sarebbero dovuti comunicare, al fine di ostacolare l'esercizio delle funzioni di vigilanza.

Le fattispecie di corruzione tra privati (art. 25-ter, comma 1, lettera s-bis, del D. Lgs. n. 231/2001) La Legge 6 novembre 2012, n. 190, recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", ha introdotto nel nostro ordinamento il reato di corruzione tra privati, attraverso la modifica dell'art. 2635 c.c. – prima rubricato "infedeltà a seguito di dazione o promessa di utilità"

L'Articolo oggi recita come segue:

Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per se' o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.
Chi, anche per interposta persona, offre, promette o da' denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste.
Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.
Fermo quanto previsto dall'articolo 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse o offerte.

Istigazione alla corruzione tra privati (art. 2635-bis c.c.) Il D. Lgs. n. 38/2017 ha introdotto nell'ordinamento una nuova fattispecie di reato, denominata "istigazione alla corruzione tra privati" prevista e punita dall'art. 2635-bis c.c.
L'Articolo oggi recita come segue:
Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata".
Ai sensi dell'art. 2639 c.c., per i reati societari sopra descritti, al soggetto formalmente investito della qualifica o titolare della funzione prevista dalla legge civile (c.d. reati propri) è equiparato sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti a tale qualifica o funzione.

3.3. Attività aziendali sensibili

Con specifico riferimento ai reati societari ai fini della presente Parte Speciale stante la natura di Sede Secondaria della sede italiana Younited si evidenziano:

- Gestione dell'informativa periodica;
- Gestione dei rapporti con le Autorità di Vigilanza

3.4. Gestione dell'informativa periodica

Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Sede Secondaria.
La Sede Secondaria italiana di Younited S.A., in quanto succursale di una banca estera, non è soggetta all'obbligo di deposito del bilancio in Italia, ai sensi delle disposizioni normative vigenti.
Tuttavia, al fine di garantire il corretto adempimento degli obblighi fiscali nazionali, viene comunque predisposto un bilancio a fini fiscali, necessario per il calcolo e il versamento delle imposte sul reddito d'impresa e dell'IRAP.
Ai sensi del D. Lgs. n. 231/2001, il processo di predisposizione dei documenti in oggetto potrebbe presentare occasioni per la commissione del reato di "*false comunicazioni sociali*", così come disciplinato agli artt. 2621 e 2622 del Codice Civile nonché i reati tributari, definiti nel paragrafo 6.
La predisposizione del bilancio fiscale italiano della Sede Secondaria avviene con il supporto di una società di revisione esterna, che assiste anche nella predisposizione del bilancio consolidato del Gruppo Younited.
Le informazioni contabili necessarie per la redazione del bilancio fiscale vengono trasmesse dalla Casa Madre francese, che gestisce centralmente la contabilità e i flussi informativi finanziari.
Inoltre, le regole aziendali e i controlli di completezza e di veridicità previsti nel presente protocollo sono predisposti anche al fine di una più ampia azione preventiva dei reati che potrebbero conseguire a una scorretta gestione delle risorse finanziarie, quali i reati di "*corruzione*", nelle loro varie tipologie, di "*induzione indebita*", di "*corruzione tra privati*" e di "*istigazione alla corruzione tra privati*", nonché i reati di "*riciclaggio*" e di "*autoriciclaggio"*.
Inoltre, tale processo è posto a presidio dei reati societari di illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.), operazioni in pregiudizio dei creditori (art. 2629 c.c.), formazione fittizia del capitale (art. 2632 c.c.).
Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.
Il presente protocollo è predisposto al fine di garantire, anche per le attività di predisposizione del bilancio fiscale e di comunicazione finanziaria verso la Casa Madre e verso gli organi competenti, un presidio costante di correttezza, trasparenza e tracciabilità delle informazioni economico-patrimoniali

3.5. Descrizione del Processo

Nell'ambito dei processi sensibili ai fini dell'informativa finanziaria, particolare rilievo assumono le attività strettamente funzionali alla produzione del bilancio d'esercizio, delle situazioni contabili infrannuali e l'alimentazione del *reporting package* per il bilancio consolidato del Gruppo la determinazione degli oneri fiscali e lo svolgimento degli adempimenti relativi alle imposte dirette ed indirette.

Tali attività attengono ai seguenti processi aziendali:

- Gestione della contabilità e delle segnalazioni di vigilanza;
- Gestione del bilancio d'impresa, e del reporting package per il bilancio consolidato del Gruppo;
- Gestione delle operazioni societarie.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

3.6. Principi di controllo

I documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Sede Secondaria devono essere redatti in base alle specifiche procedure, prassi e logiche aziendali e di Gruppo in essere che:

- identificano con chiarezza e completezza le funzioni interessate nonché i dati e le notizie che le stesse devono fornire;
- identificano i criteri per le rilevazioni contabili dei fatti aziendali, inclusa la valutazione delle singole poste;
- determinano le scadenze, gli argomenti oggetto di comunicazione e informativa, l'organizzazione dei relativi flussi e l'eventuale richiesta di rilascio di apposite attestazioni;
- prevedono la trasmissione di dati ed informazioni alla Struttura responsabile della raccolta attraverso un sistema che consente la tracciabilità delle singole operazioni e l'identificazione dei soggetti che inseriscono i dati nel sistema;

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Ruoli e responsabilità definiti:
  - ogni singola Struttura è responsabile dei processi che contribuiscono alla produzione delle voci contabili e/o delle attività valutative ad essa demandate e degli eventuali commenti in bilancio di propria competenza;
  - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in relazione alle attività in oggetto, in particolare per quanto riguarda il passaggio a perdite;
  - sono definiti diversi profili di utenza per l'accesso alle procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
  - la verifica dell'adeguatezza dei processi sensibili ai fini della informativa contabile e finanziaria nonché dei relativi controlli è affidata ad una specifica struttura della funzione Amministrazione che rappresenta altresì l'interfaccia del Servizio di Governance Amministrativo Finanziaria della Casa Madre con il quale si coordina per la redazione dei documenti contabili e societari ed alla funzione Internal Audit nell'ambito dello svolgimento della sua attività.
- Segregazione delle funzioni:
  - il processo di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Sede Secondaria prevede il coinvolgimento di distinte Strutture, operanti nelle diverse fasi del processo

- Attività di controllo:
  - le attività di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Sede Secondaria sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali. Si riportano nel seguito i principali controlli svolti dalle singole Strutture:
    - verifiche, con cadenza periodica, dei saldi dei conti di contabilità generale, al fine di garantirne la quadratura con i rispettivi partitari;
    - verifica, con periodicità prestabilita, di tutti i saldi dei conti lavorazione, transitori e similari, per assicurare che le Unità interessate che hanno alimentato la contabilità eseguano le necessarie scritture nei conti appropriati;
    - esistenza di controlli maker e checker attraverso i quali la persona che esegue l'operazione è differente da quella che la autorizza, previo controllo di adeguatezza;
    - produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
    - analisi degli scostamenti, attraverso il confronto tra i dati contabili esposti nel periodo corrente e quelli relativi a periodi precedenti;
    - controllo di merito in sede di accensione di nuovi conti ed aggiornamento del piano dei conti;
    - quadratura della versione definitiva del bilancio con i dati contabili.
      - La verifica dell'adeguatezza dei processi sensibili ai fini dell'informativa contabile e finanziaria e dell'effettiva applicazione dei relativi controlli è articolata nelle seguenti fasi:
        - verifica del disegno dei controlli;
        - test dell'effettiva applicazione dei controlli;
        - identificazione delle criticità e dei piani di azione correttivi;
        - monitoraggio sull'avanzamento e sull'efficacia delle azioni correttive intraprese.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - il processo decisionale, con riferimento alle attività di predisposizione dei documenti che contengono comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Sede Secondaria è garantito dalla completa tracciabilità di ogni operazione contabile sia tramite sistema informatico sia tramite supporto cartaceo;
  - tutte le scritture di rettifica effettuate dalle singole Strutture responsabili dei conti di propria competenza sono supportate da adeguata documentazione dalla quale sia possibile desumere i criteri adottati e, analiticamente, lo sviluppo dei relativi calcoli;
  - tutta la documentazione relativa ai controlli periodici effettuati viene archiviata presso ciascuna Struttura coinvolta per le voci contabili di propria competenza;
  - tutta la documentazione di supporto alla stesura del bilancio è archiviata presso la Struttura deputata alla gestione del Bilancio e/o presso le strutture coinvolte nel processo di redazione delle disclosure.

3.7. Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nelle attività di tenuta della contabilità e della successiva predisposizione/deposito delle comunicazioni sociali in merito alla situazione economico e patrimoniale della Sede Secondaria (bilancio di esercizio, relazione sulla gestione, relazioni trimestrali e semestrali, ecc.) e del Gruppo (reporting package per il bilancio consolidato) sono tenute ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia e nelle procedure che disciplinano le attività in questione, norme tutte improntate a principi di trasparenza, accuratezza e completezza delle informazioni contabili al fine di produrre situazioni economiche, patrimoniali e finanziarie veritiere e tempestive anche ai sensi ed ai fini di cui agli artt. 2621 e 2622 del Codice Civile. In particolare, le Strutture della Sede Secondaria coinvolte nel processo sono tenute a:

- rappresentare i fatti di gestione in modo corretto, completo e tempestivo nella contabilità e nei dati aziendali allo scopo di garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari della Sede Secondaria;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Sede Secondaria.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Sede Secondaria;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Sede Secondaria.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

3.8. Gestione dei rapporti con le Autorità di Vigilanza

3.8.1 Premessa

La gestione dei rapporti con le Autorità di Vigilanza costituisce un'attività sensibile ai fini del Modello 231, in quanto implica la gestione di flussi informativi verso soggetti istituzionali e il rispetto di obblighi regolamentari che possono

rilevare sotto il profilo della responsabilità amministrativa degli enti. Per Younited S.A. – Sede Secondaria italiana, l'Autorità di riferimento principale è la Banca d'Italia. La corretta gestione dei rapporti con l'Autorità è fondamentale per garantire trasparenza, tracciabilità e conformità alle normative vigenti.

3.8.2 Descrizione del processo

La gestione dei rapporti con le Autorità di Vigilanza si articola nelle seguenti attività:

- La responsabilità operativa è affidata alla Funzione Compliance & Regulatory Affairs, in coordinamento con la Direzione Generale.
- Sono previsti due incontri fissi all'anno con la Banca d'Italia. Ulteriori interazioni (riunioni o richieste documentali) avvengono su iniziativa dell'Autorità.
- L'unica ispezione subita fino ad oggi ha riguardato il tema della trasparenza bancaria; non sono state ricevute altre richieste ispettive.
- È stata predisposta una procedura interna operativa, che disciplina:
  - i flussi informativi verso la Banca d'Italia (es. Centrale dei Rischi, Segnalazioni di Vigilanza);
  - le modalità di invio e i contenuti obbligatori, descritti in un manuale operativo allegato alla procedura.
- La procedura sarà periodicamente aggiornata per recepire eventuali modifiche normative.

3.8.3 Principi di controllo

I controlli previsti sul processo sono:

- Gestione dei rapporti con l'Autorità affidata a un soggetto specifico: la Funzione Compliance & Regulatory Affairs, sotto il coordinamento della Direzione Generale.
- Predisposizione di una procedura interna formalizzata e operativa, che regola i flussi informativi verso la Banca d'Italia.
- Archiviazione e tracciabilità di tutti i contatti con l'Autorità mediante:
  - repository dedicato, accessibile alla Funzione Compliance e all'Organismo di Vigilanza;
  - protocollo della corrispondenza, per garantire la tracciabilità e la tempestività delle risposte.
- Manuale operativo allegato alla procedura per garantire la corretta gestione dei contenuti da trasmettere e dei canali utilizzati.

3.8.4 Principi di comportamento

I soggetti coinvolti nella gestione dei rapporti con le Autorità di Vigilanza devono:

- rispettare la procedura interna;
- assicurare che tutte le informazioni trasmesse siano complete, veritiere e tempestive;
- garantire la protocollazione e l'archiviazione di tutta la documentazione scambiata con l'Autorità;

- mantenere un comportamento di collaborazione e trasparenza nei confronti della Banca d'Italia e delle altre Autorità eventualmente competenti;
- segnalare tempestivamente eventuali richieste o criticità all'Organismo di Vigilanza.

3.9. I FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.

I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.
- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua verifiche semestrali, ad evento e annuali.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	**Descrizione del flusso informativo**	**Periodicità**
Finance & Accounting	Comunicazione di eventuali rilievi del revisore contabile o dell'Agenzia delle Entrate relativi alla redazione del bilancio e della contabilità.	Ad evento
Finance & Accounting	Trasmissione della bozza di bilancio d'esercizio locale.	Annuale
Compliance & Regulatory Affairs	Informativa su richieste, note o verbali ispettivi delle Autorità e stato di avanzamento delle azioni correttive.	Ad evento
Corporate Affairs	Invio verbali assembleari, del CdA e della Capogruppo relativi ad operazioni sul capitale, fusioni, scissioni.	Ad evento
Internal Audit	Report di audit inerenti ai processi contabili e ai rischi di reato societario.	Semestrale

4. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E IL SUO PATRIMONIO, REATI DI INTRALCIO ALLA GIUSTIZIA

4.1. Premessa

La presente Parte Speciale ha l'obiettivo di illustrare i criteri, i ruoli e le responsabilità, i principi di controllo e le regole di comportamento cui tutti i Destinatari, ivi compresi i consulenti, i dipendenti, i fornitori e i partner, devono attenersi nella gestione dei Processi a Rischio connessi con le fattispecie di reato previste dagli articoli 24, 25, 25-*decies* e 25-*duodecies* del Decreto, nel rispetto dei principi di legalità, correttezza, oggettività, trasparenza, tracciabilità e riservatezza nell'esecuzione delle proprie attività, della normativa emanata dagli organismi di vigilanza e di tutte le leggi e le norme nazionali ed internazionali vigenti.
Quanto definito nella presente Parte Speciale si applica a tutte le Unità Organizzative coinvolte nei Processi a Rischio di seguito elencati nonché alle funzioni di controllo deputate a vigilare sul rispetto e l'adeguatezza delle procedure applicabili in materia di prevenzione dei reati nei confronti della Pubblica Amministrazione (come infra definita) e del suo patrimonio e dei reati di intralcio alle attività dell'autorità giudiziaria.

4.2. CRITERI PER LA DEFINIZIONE DI P.A. E DI SOGGETTI INCARICATI DI UN PUBBLICO SERVIZIO

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire un elenco esemplificativo dai soggetti di cui all'articolo 5, comma 1, lett. a) e b), D.Lgs. n. 231/2001.
Sono, inoltre, riportate anche delle indicazioni in merito alle fattispecie di reato che si possono compiere in relazione alle diverse categorie di soggetti coinvolti.

Enti della pubblica amministrazione

Agli effetti della legge penale, viene comunemente considerato come "Ente della pubblica amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.
Sebbene non esista nel Codice Penale una definizione di pubblica amministrazione, in base a quanto stabilito nella Relazione Ministeriale al codice stesso ed in relazione ai reati in esso previsti, sono ritenuti appartenere alla pubblica amministrazione quegli enti che svolgano "tutte le attività dello Stato e degli altri enti pubblici".
Ai fini del presente documento si intendono per "Pubblica Amministrazione", in via esemplificativa:

- i soggetti pubblici, ossia, i membri del Parlamento della Repubblica Italiana, le amministrazioni pubbliche, quali le amministrazioni dello Stato, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni e i loro consorzi e associazioni, le istituzioni universitarie, le Camere di Commercio, Industria, Artigianato e Agricoltura, gli enti pubblici non

economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del servizio sanitario nazionale;
- gli enti pubblici produttori di servizi economici, gli enti pubblici produttori di servizi assistenziali, ricreativi e culturali e gli enti di ricerca;
- gli enti pubblici previdenza e assistenza sociale (es. INPS, INAIL, ENPAM, INARCASSA, Cassa del Notariato, ecc. L'elenco completo può essere reperito sul sito internet dell'ISTAT richiamato sopra in nota);
- i pubblici ufficiali, ossia coloro che, pubblici dipendenti o privati, possano o debbano formare e manifestare la volontà della pubblica amministrazione, ovvero esercitare poteri autoritativi o certificativi, nell'ambito di una potestà di diritto pubblico;
- gli incaricati di pubblico servizio, ossia coloro che prestano un servizio pubblico ma non sono dotati dei poteri del pubblico ufficiale ovvero che, pur agendo nell'ambito di un'attività disciplinata nelle forme della pubblica funzione, non esercitano i poteri tipici di questa e non svolgono semplici mansioni d'ordine né prestano opera meramente materiale;
- le Autorità pubbliche di Vigilanza, ossia, quegli enti dotati di particolare autonomia e imparzialità il cui obiettivo è la tutela di alcuni interessi di rilievo costituzionale, quali il buon andamento della Pubblica Amministrazione, la libertà di concorrenza, la tutela della sfera di riservatezza professionale, la tutela dei mercati finanziari ecc.

In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio".

Pubblici Ufficiali e Incaricati di Pubblico Servizio

Ai sensi dell'articolo 357, primo comma Cod. Pen. è considerato pubblico ufficiale "*agli effetti della legge penale*" colui il quale esercita "*una pubblica funzione legislativa, giudiziaria o amministrativa*".

Il secondo comma si preoccupa poi di definire la nozione di "pubblica funzione amministrativa". Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*".

Inoltre, il secondo comma dell'articolo 357 Cod. Pen. traduce in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di "pubblica funzione" da quella di "servizio pubblico". Vengono quindi pacificamente definite come "funzioni pubbliche" quelle attività amministrative che rispettivamente ed alternativamente costituiscono esercizio di: (a) poteri deliberativi; (b) poteri autoritativi; (c) poteri certificativi. Alla luce dei principi sopra enunciati, si può affermare che la categoria di soggetti più problematica è certamente quella che ricopre una "pubblica funzione amministrativa".

In sintesi, può dirsi che la distinzione tra le due figure è in molti casi controversa e labile e che la stessa è definita dalle predette norme secondo criteri basati sulla funzione oggettivamente svolta dai soggetti in questione. La qualifica di Pubblico Ufficiale è attribuita a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. L'esercizio di una pubblica funzione amministrativa solitamente è riconosciuto sussistere in capo a coloro che formano o concorrono a formare la volontà dell'ente pubblico o comunque lo rappresentano di fronte ai terzi, nonché a coloro che sono muniti di poteri autoritativi o certificativi12.
La qualifica di Incaricato di Pubblico Servizio si determina per via di esclusione, spettando a coloro che svolgono quelle attività di interesse pubblico, non consistenti in semplici mansioni d'ordine o meramente materiali, disciplinate nelle stesse forme della pubblica funzione, ma alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale.

A titolo esemplificativo si elencano i seguenti soggetti nei quali la giurisprudenza ha individuato la qualifica di Incaricato di Pubblico Servizio: esattori dell'Enel, letturisti dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento della corrispondenza, dipendenti del Poligrafico dello Stato, guardie giurate che conducono furgoni portavalori. Va considerato che la legge non richiede necessariamente, ai fini del riconoscimento in capo ad un determinato soggetto delle qualifiche pubbliche predette, la sussistenza di un rapporto di impiego con un Ente pubblico: la pubblica funzione od il pubblico servizio possono essere esercitati, in casi particolari, anche da un privato.
Deve porsi particolare attenzione al fatto che, ai sensi dell'art. 322-bis c.p., la condotta del soggetto privato - sia esso corruttore o indotto a dare o promettere utilità - è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri, Organizzazioni pubbliche internazionali o sovranazionali, Assemblee parlamentari internazionali, Corti internazionali.

4.3. Fattispecie di reato previste dagli artt. 24, 25 e 25-*decies* e 25-*duodecies* del Decreto

Tra le fattispecie penali qui considerate, i reati di concussione e di induzione indebita a dare o promettere utilità nonché i reati di "corruzione", nelle loro varie tipologie, presuppongono il coinvolgimento necessario di un soggetto privato e di un pubblico agente, vale a dire 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. e secondo quanto indicato nel punto precedente.

Si illustrano sinteticamente qui di seguito le fattispecie delittuose previste dagli artt. 24 e 25 del Decreto.

Malversazione a danno dello Stato (art. 316-bis c.p.) Tale ipotesi di reato si configura nel caso in cui, chiunque estraneo alla pubblica amministrazione, dopo avere ricevuto finanziamenti, contributi, sovvenzioni, mutui agevolati ovvero altre erogazioni dello stesso tipo comunque denominate da parte dello Stato italiano, da altro ente pubblico o dell'Unione Europea, non proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).
Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.
Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.) La fattispecie criminosa si realizza 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 dalle Comunità Europee.
In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. È previsto un aumento di pena il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.
Frode nelle Pubbliche Forniture (art. 346 c.p.) La norma in parola prevede la punizione di chiunque commette frode nella esecuzione dei contratti di forniture o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo 355 c.p. è punito con la reclusione da uno a cinque anni e con la multa non inferiore a 1.032 euro.
Truffa ai danni dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1, c.p.) Tale ipotesi di reato si configura nel caso in cui si ottenga un ingiusto profitto ponendo in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato oppure ad altro Ente Pubblico.
La condotta consiste, sostanzialmente, in qualsiasi tipo di menzogna (compreso l'indebito silenzio su circostanze che devono essere rese note) tramite la quale si ottiene che taluno cada in errore su qualcosa e compia, di conseguenza, un atto di disposizione che non avrebbe compiuto se avesse conosciuto la verità. Per la consumazione del reato occorre che sussista, oltre a tale condotta, il conseguente profitto di qualcuno (chiunque esso sia, anche diverso dall'ingannatore) e il danno dello Stato o dell'ente pubblico.
Il reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni supportate da documentazione artefatta, al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.) Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni da parte dello Stato, di altro Ente pubblico o delle Comunità Europee.
Gli elementi caratterizzanti il reato in esame sono: rispetto al reato di truffa generica (art. 640, comma 2, n. 1, c.p.), l'oggetto materiale specifico, che per la presente fattispecie consiste nell'ottenimento di erogazioni pubbliche comunque denominate; rispetto al reato di indebita percezione di erogazioni (art. 316-ter c.p.), la necessità dell'ulteriore elemento della attivazione di artifici o raggiri idonei ad indurre in errore l'ente erogante.
Frode informatica (art. 640-ter c.p.) La fattispecie di frode informatica consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati o programmi in essi contenuti, ottenendo un ingiusto profitto. Essa assume rilievo ai fini del D. Lgs. n. 231/2001, soltanto nel caso in cui sia perpetrata ai danni dello Stato o di altro Ente Pubblico.
In concreto, può integrarsi il reato in esame qualora, ad esempio, una volta ottenuto un finanziamento, fosse violato un sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente, oppure anche nel caso di modificazione delle risultanze di un conto corrente intestato ad un ente pubblico, abusivamente accedendo a un sistema di home banking.
Concussione (art. 317 c.p.) Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o l'incaricato di un pubblico servizio, abusando della sua qualità o dei suoi poteri, costringa taluno a dare o a promettere indebitamente a sé o ad altri denaro o altre utilità.
Tuttavia, a differenza della corruzione, solo il concussore è assoggettato a pena, in quanto il concusso è la vittima del reato: pertanto, per la natura privatistica dell'attività svolta dalla Società, i suoi esponenti non potrebbero commettere il reato in proprio in quanto sprovvisti della necessaria qualifica pubblicistica; i medesimi potrebbero tutt'al più concorrere in un reato di concussione commesso da un pubblico ufficiale o da un incaricato di pubblico servizio ai sensi dell'art. 110 c.p. Inoltre, è astrattamente possibile che un dipendente della Società rivesta, al di fuori dell'attività lavorativa, una pubblica funzione o svolga un pubblico servizio: si pensi al dipendente della Società che svolga l'incarico di componente di una giunta comunale. In tale ipotesi, questi, nello svolgimento del proprio ufficio o servizio, dovrà astenersi dal tenere comportamenti che, in violazione dei propri doveri d'ufficio e/o con abuso delle proprie funzioni, siano idonei a recare un vantaggio alla Società. Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
Il reato punisce la condotta dell'Incaricato di Pubblico Servizio o del Pubblico Ufficiale che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere a lui o a un terzo denaro o altre utilità non dovutegli.
Si tratta di fattispecie diversa da quella di concussione: le pressioni e richieste del pubblico agente non sono tali da esercitare la violenza morale tipica dell'estorsione, ma assumono forme di mero condizionamento della volontà della controparte, quali prospettazioni di possibili conseguenze sfavorevoli o difficoltà, ostruzionismi, ecc. È punita anche la condotta della persona che cede all'induzione, corrispondendo o promettendo l'indebita utilità per evitare un

danno o conseguire un vantaggio illecito.
Pertanto, la responsabilità degli enti a titolo di induzione indebita è configurabile, sempre che sussista l'interesse o vantaggio dell'ente, nel caso di reato commesso da un soggetto apicale o da un subordinato secondo una delle seguenti forme alternative:

- condotta induttiva posta in essere in concorso con un Pubblico Ufficiale o con un Incaricato di Pubblico Servizio nei confronti di un terzo;
- condotta induttiva tenuta nell'esercizio di talune attività di rilevanza pubblica che possono comportare l'assunzione in capo all'operatore della qualifica di pubblico ufficiale o di incaricato di pubblico servizio;
- accettazione delle condotte induttive provenienti da un pubblico ufficiale o da un incaricato di pubblico servizio.

Corruzione
L'elemento comune a tutte le varie fattispecie del reato di corruzione contro la Pubblica Amministrazione consiste nell'accordo fra un pubblico ufficiale o un incaricato di pubblico servizio e un soggetto privato. L'accordo corruttivo presuppone che le controparti agiscano in posizione paritaria fra di loro e non ha rilevanza il fatto che l'iniziativa provenga dall'una o dall'altra parte, diversamente da quanto avviene nei reati di concussione e di induzione indebita a dare o promettere utilità, che invece richiedono che il soggetto rivestente la qualifica pubblica paventando l'abuso dei propri poteri, faccia valere la propria posizione di superiorità, alla quale corrisponde nel privato una situazione di soggezione. Peraltro, può risultare difficile distinguere nella pratica quando ricorra una fattispecie di corruzione piuttosto che un reato di induzione indebita; la distinzione rileva innanzitutto per la determinazione della pena con la quale è punito il soggetto privato, che è più lieve nel reato di induzione indebita.

Nel fatto della corruzione si ravvisano due distinti reati: l'uno commesso dal soggetto corrotto, rivestente la qualifica pubblica (c.d. corruzione passiva), l'altro commesso dal corruttore (c.d. corruzione attiva), che - in forza della disposizione di cui all'art. 321 c.p. - è punito con le stesse pene previste per il corrotto.
Le fattispecie di corruzione previste dall'art. 25 del Decreto sono le seguenti.
Corruzione per l'esercizio della funzione (art. 318 c.p.) Tale ipotesi di reato si configura nel caso in cui un Pubblico Ufficiale o un Incaricato di Pubblico Servizio riceva, per sé o per o per un terzo, denaro o altra utilità, o ne accetti la promessa, per l'esercizio delle sue funzioni o dei suoi poteri. L'attività del pubblico agente può estrinsecarsi in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), ma il reato sussiste anche se l'utilità indebita è:

- corrisposta o promessa a prescindere dall'individuazione della "compravendita" di un atto ben determinato, in quanto è sufficiente il solo fatto che sia posta in relazione col generico esercizio della funzione;
- corrisposta dopo il compimento di un atto d'ufficio, anche se precedentemente non promessa.

Rilevano quindi ipotesi di pericolo di asservimento della funzione ampie e sfumate e dazioni finalizzate a una generica aspettativa di trattamento favorevole13.
Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) Il reato, detto anche di "corruzione propria", consiste in un accordo per la promessa o dazione di un indebito compenso riferito ad un atto, da compiersi o già compiuto,

contrario ai doveri del pubblico agente (ad esempio: corresponsione di denaro per garantire l'aggiudicazione di una gara).

Corruzione in atti giudiziari (art. 319-ter, comma 1, c.p.) Tale ipotesi di reato si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso (non espressamente contemplato nella norma), si corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario). Tale fattispecie si realizza anche quando il vantaggio sia ottenuto a favore di una società che non sia parte del procedimento.

Istigazione alla corruzione (art. 322 c.p.) Tale reato è commesso dal soggetto privato la cui offerta o promessa di denaro o di altra utilità per l'esercizio di funzioni pubbliche (art. 318 c.p.) o di un atto contrario ai doveri d'ufficio (art. 319 c.p.) non sia accettata. Per il medesimo titolo di reato risponde il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio che solleciti, con esito negativo, tale offerta o promessa**.**

Traffico di influenze illecite (art. 346-bis c.p.)[1]

Commette il reato chi, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio - o con i soggetti che esercitano corrispondenti funzioni nell'ambito dell'Unione Europea, di Paesi terzi, di Organizzazioni o di Corti internazionali - indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso tali soggetti, ovvero per remunerarli in relazione all'esercizio delle loro funzioni. È punito allo stesso modo dell'intermediario anche il soggetto che con lui si accorda per l'effettuazione delle illecite influenze. Sono previste aggravanti di pena per i casi in cui il "venditore" di relazioni influenti, vere o vantate, rivesta la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio, o per i casi in cui si prefiguri un'influenza sull'esercizio di attività giudiziarie, oppure il fine di remunerare un pubblico ufficiale o un incaricato di pubblico servizio per il compimento di un atto contrario ai doveri d'ufficio o per l'omissione o il ritardo di un atto d'ufficio.

Per integrare il reato non occorre che l'influenza illecita sia effettivamente esercitata; nel caso in cui ciò avvenisse e sussistessero gli estremi dei reati di corruzione di cui agli articoli 318, 319, 319-ter sopra illustrati, le parti dell'accordo illecito verrebbero punite non ai sensi dell'art. 346- bis, ma a titolo di concorso nella commissione di detti reati. Si tratta quindi di un reato che intende prevenire e punire anche il solo pericolo di eventuali accordi corruttivi.

La norma punisce anche la mediazione per l'esercizio della funzione pubblica - cioè per il compimento di atti non contrari ai doveri d'ufficio - che potrebbe preludere ad accordi corruttivi puniti dall'art. 318 c.p. Si può però ritenere che siano legittime le attività di rappresentazione dei propri interessi (cosiddette attività di lobbying) o delle proprie ragioni difensive alle competenti autorità mediante associazioni di categoria o professionisti abilitati, purché siano svolte in modo trasparente e corretto e non per ottenere indebiti favori.

Corruzione Di Persona Incaricata Di Un Pubblico Servizio (Art. 320 c.p.)

Tale ipotesi di reato si configura nel caso in cui un incaricato di pubblico servizio

[1] Il reato di traffico di influenze illecite è stato introdotto nel codice penale dalla L. n. 190/2012 e poi modificato dalla L. n. 3/2019, che lo ha aggiunto ai reati presupposto previsti dall'art. 25 del D. Lgs. n. 231/2001, con effetto dal 31.1.2019.

riceva (o ne accetti la promessa), per sé o per altri, denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri o per omettere o ritardare un atto del suo ufficio ovvero per compiere un atto contrario al suo dovere d'ufficio.

Turbata Libertà Degli Incanti (Art. 353 c.p.)

Tale ipotesi di reato sanziona la condotta di chiunque, con violenza o minaccia, o doni, promesse, collusioni o altri mezzi, impedisce, turba, o allontana i partecipanti da una gara nei pubblici incanti o nelle licitazioni private per conto delle pubbliche amministrazioni.

La fattispecie in esame ha come finalità quella di tutelare la fase di formazione dell'attività negoziale della Pubblica Amministrazione, con specifico riguardo alla scelta dei contraenti nonché al rispetto delle regole volte a disciplinare le gare pubbliche ovvero le licitazioni private.

A tal riguardo, si precisa che:

a) la gara è una forma di scelta del contraente della Pubblica Amministrazione che avviene tramite un processo formale o una libera competizione, anche informale o ufficiosa, nel cui ambito siano previamente indicati e resi noti i criteri di selezione delle offerte;

b) la licitazione privata, diretta da un pubblico ufficiale o da persona legalmente autorizzata, è una gara che non si rivolge al pubblico, bensì a più concorrenti selezionati dalla Pubblica Amministrazione.

Tale reato può realizzarsi non solo nel momento in cui la gara si svolge, ma anche nelle fasi antecedenti o prodromiche alla stessa, purché sia già stato pubblicato il bando di gara o un altro atto equipollente.

Il reato si consuma qualora si sia realizzato l'impedimento (allontanamento) o la turbativa della gara (modifica delle condizioni della stessa), ovvero l'allontanamento degli offerenti.

Turbata Libertà Del Procedimento Di Scelta Del Contraente (Art. 353-Bis c.p.)

Tale ipotesi di reato sanziona la condotta di chi, con violenza, minaccia, doni, promesse, collusioni o altri mezzi fraudolenti, turba il procedimento amministrativo mediante il quale è stabilito il contenuto del bando o di altro atto equipollente, al fine di condizionare il procedimento amministrativo di scelta del contraente da parte della Pubblica Amministrazione. Il reato sanziona, quindi, le condotte poste in essere nella fase di indizione della gara e segnatamente nell'ambito del processo diretto a stabilire il contenuto del bando.

4.4. Le Attività Aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere comportamenti illeciti nei rapporti con la Pubblica Amministrazione sono le seguenti:

- Gestione dei rapporti contrattuali con la Pubblica Amministrazione;
- Gestione delle attività inerenti alla richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione della formazione finanziata: richiesta, ottenimento e gestione di fondi pubblici per finanziare la formazione del personale;
- Gestione e utilizzo dei sistemi informativi e del Patrimonio Informativo della Società;

Gestione dei contenziosi e degli accordi transattivi;

- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del processo di selezione e assunzione del personale;
-
- Gestione dei rapporti con i Regolatori e Autorità di Vigilanza.

Con riferimento all'attività sensibile concernente la Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Younited si rimanda al protocollo riferito ai Reati di Criminalità Informatica;
Si riportano qui di seguito, i protocolli che dettano i principi di controllo e i principi di comportamento applicabili alle altre sopraelencate attività sensibili e che si completano con la normativa aziendale di dettaglio che regolamenta le attività medesime.
Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalla Sede Secondaria, società del Gruppo e/o outsourcer esterni.

4.5. Gestione dei rapporti contrattuali con la Pubblica Amministrazione

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione delle attività aziendali.
La Società, non intrattenendo rapporti contrattuali diretti con Enti della Pubblica Amministrazione, adotta il presente protocollo, ai sensi del D. Lgs. n. 231/2001, quale misura preventiva volta a ridurre il rischio di condotte illecite riconducibili a reati contro la Pubblica Amministrazione. A titolo esemplificativo, rientrano in tale ambito: corruzione nelle diverse forme, induzione indebita a dare o promettere utilità, traffico di influenze illecite, concussione e truffa ai danni dello Stato o di altri enti pubblici.
Il presente protocollo è finalizzato a garantire che le attività aziendali si svolgano nel rispetto della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità, con particolare riferimento alla prevenzione dei reati presupposto contemplati dal Decreto.

4.5.1 Principi Di Controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori.

Livelli autorizzativi definiti. In particolare:
- La gestione dei rapporti contrattuali della Società è organizzata in modo da garantire che le relazioni con terzi siano presidiate da specifiche strutture aziendali incaricate della erogazione dei prodotti e/o servizi. La stipula di contratti con soggetti terzi deve avvenire nel rispetto dei principi di

comportamento sanciti dal presente Modello Organizzativo e, in particolare, tutti gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto da soggetti espressamente autorizzati.

- nell'ambito di ogni struttura, i soggetti che esercitano poteri autorizzativi e/o negoziali:
  - sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale o tramite delega formale da parte del Responsabile della Struttura di riferimento;
  - operano esclusivamente nell'ambito delle competenze loro attribuite;
  - sono definiti profili di utenza per l'accesso ai sistemi informatici, coerenti con le funzioni e i poteri loro assegnati.

Segregazione dei compiti tra i soggetti coinvolti nei processi di gestione dei rapporti contrattuali. In particolare:

- i soggetti deputati alla predisposizione della documentazione contrattuale sono differenti da coloro che la sottoscrivono;
- le strutture incaricate della gestione operativa dei prodotti/servizi sono diverse da quelle incaricate dello sviluppo commerciale.

Attività di controllo: la normativa interna prevede controlli di linea che devono essere svolti da ciascuna Struttura coinvolta nelle attività amministrative, contabili e operative. Deve essere garantita la verifica della regolarità delle operazioni, nonché della completezza, correttezza e tempestività delle scritture contabili, con applicazione di meccanismi di maker-checker.

Tracciabilità del processo, sia a livello di sistema informativo sia in termini documentali:

- l'esecuzione delle attività prevede l'uso di sistemi informatici che garantiscano la tracciabilità delle informazioni elaborate;
- le Strutture aziendali provvedono alla conservazione ordinata della documentazione, anche in formato elettronico, al fine di assicurare la ricostruzione delle responsabilità e la trasparenza dei processi.

Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione adottati dalla Società devono essere coerenti con le disposizioni di legge, i principi del Modello Organizzativo e le previsioni del Codice Etico, e devono prevedere idonei meccanismi correttivi in caso di comportamenti non conformi.

4.5.2 Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione derivanti da adempimenti di natura

contrattuale con gli Enti stessi, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento.
In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Sede Secondaria devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/esecuzione dei rapporti contrattuali con la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore in ordine alla scelta di attribuzione di incarichi alla Sede Secondaria;
- chiedere o indurre - anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Sede Secondaria;
- promettere o versare/offrire - anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a soggetti della Pubblica Amministrazione con la finalità di promuovere o favorire interessi della Sede Secondaria. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, e tutte le operazioni che comportino la generazione di una perdita per la Sede Secondaria e la creazione di un utile per i soggetti predetti (es. stralcio ingiustificato di posizione debitoria e/o applicazioni di sconti o condizioni non

in linea con i parametri di mercato);
- ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite dalla Sede Secondaria o, comunque, un trattamento più favorevole di quello dovuto;
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico; ciò al fine di prevenire il rischio di commissione di reati di "corruzione" nelle loro varie tipologie, e di "induzione indebita a dare o promettere utilità" e di "traffico di influenze illecite" che potrebbero derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Sede Secondaria.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

4.6. Gestione delle attività inerenti alla richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione

4.6.1 Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione delle attività inerenti alla richiesta di autorizzazioni, all'esecuzione di adempimenti e agli obblighi informativi verso gli Enti Regolatori, quali, a titolo esemplificativo e non esaustivo:
- gestione dei rapporti con Banca d'Italia per l'ottenimento e il mantenimento delle autorizzazioni necessarie a operare nel settore del credito istantaneo, nonché per l'esecuzione di adempimenti connessi (es. riserva obbligatoria, segnalazioni periodiche, vigilanza prudenziale);
- gestione dei rapporti con Agenzia delle Entrate per l'esecuzione di adempimenti fiscali e tributari previsti dalla normativa vigente;
- gestione dei rapporti con altre Autorità di Vigilanza o Regolatorie (es. AGCM, Garante per la protezione dei dati personali) per il rispetto della normativa di settore, incluse le disposizioni in materia di privacy e concorrenza;
- gestione degli adempimenti presso le Camere di Commercio e il Registro delle Imprese per le attività obbligatorie di iscrizione e aggiornamento;
- gestione degli adempimenti connessi alla richiesta e all'ottenimento di certificazioni e autorizzazioni eventualmente necessarie per lo svolgimento delle attività aziendali.

La Società non intrattiene alcun tipo di rapporto contrattuale con la Pubblica Amministrazione per la fornitura di beni o servizi, limitandosi ai soli rapporti istituzionali obbligatori con gli Enti sopra indicati.

Ai sensi del D.Lgs. n. 231/2001, le attività sopra descritte potrebbero comunque

presentare occasioni per la commissione dei reati di corruzione (nelle varie tipologie previste), induzione indebita a dare o promettere utilità, traffico di influenze illecite, truffa ai danni dello Stato o di altro ente pubblico. Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

4.6.2 Descrizione del Processo

Il processo di gestione dei rapporti con la Pubblica Amministrazione in occasione di richieste di autorizzazioni o esecuzione di adempimenti si articola nelle seguenti fasi:

- predisposizione della documentazione;
- invio della documentazione richiesta e archiviazione della pratica;
- gestione dei rapporti con gli Enti pubblici;
- assistenza in occasione di sopralluoghi ed accertamenti da parte degli Enti;
- gestione dei rapporti con gli Enti pubblici per il ritiro dell'autorizzazione e l'esecuzione degli adempimenti.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

4.6.3 Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

Livelli autorizzativi definiti

- Nell'ambito di ogni Struttura, tutti i soggetti che intervengono nella gestione delle attività inerenti alla richiesta di autorizzazioni o all'esecuzione di adempimenti verso gli **Enti Regolatori** (quali Banca d'Italia, Agenzia delle Entrate, Garante Privacy, AGCM):
  - sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dalle funzioni gramma aziendale ovvero dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima; nel caso in cui i rapporti con tali Enti vengano gestiti da soggetti terzi, questi ultimi sono individuati con apposita lettera di incarico/nomina ovvero tramite specifiche clausole contrattuali;
  - operano esclusivamente nell'ambito del perimetro di attività e responsabilità loro assegnato dal Responsabile della Struttura di riferimento;
- La gestione dei rapporti con i funzionari degli Enti Regolatori in caso di accertamenti, ispezioni o richieste di informazioni è attribuita al Responsabile della Struttura e/o ai soggetti da quest'ultimo appositamente individuati.

Segregazione dei compiti tra i soggetti coinvolti nel processo di gestione delle attività inerenti alla richiesta di autorizzazioni o all'esecuzione di adempimenti

verso gli Enti Regolatori, al fine di garantire per tutte le fasi del processo un meccanismo di *maker* e *checker*.

Attività di controllo: le attività devono essere svolte in modo tale da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto delle richieste di autorizzazioni o degli adempimenti obbligatori, prevedendo, ove opportuno, specifici controlli in contraddittorio. In particolare, laddove l'autorizzazione o l'adempimento preveda l'elaborazione di dati, è effettuato un controllo sulla correttezza delle elaborazioni da parte di soggetti diversi da quelli deputati alla esecuzione delle attività.

Tracciabilità del processo, sia a livello di sistema informativo sia in termini documentali:

- copia della documentazione consegnata agli Enti Regolatori per la richiesta di autorizzazioni o per l'esecuzione di adempimenti è conservata presso l'archivio della Struttura di competenza;
- il Responsabile della Struttura o il soggetto aziendale incaricato ha l'obbligo di conservare copia dei verbali redatti dagli Enti Regolatori in occasione di eventuali accertamenti o ispezioni, unitamente ai relativi allegati;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza, prodotta anche in via telematica o elettronica, inerente all'esecuzione degli adempimenti svolti nell'ambito delle attività verso gli Enti Regolatori.

4.6.4 Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione in occasione di richiesta di autorizzazioni o esecuzione di adempimenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Sede Secondaria devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- qualora sia previsto il coinvolgimento di soggetti terzi (professionisti, ditte, ecc.) nell'espletamento delle attività inerenti alla richiesta di autorizzazioni ovvero nell'esecuzione di adempimenti verso la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la

corruzione e di impegno al loro rispetto;

- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- chiedere o indurre - anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente il riscontro da parte della Pubblica Amministrazione;
- promettere o versare/offrire - anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni al di fuori delle prassi dei regali di cortesia di modico valore e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a soggetti della Pubblica Amministrazione con la finalità di promuovere o favorire interessi della Sede Secondaria. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini la sponsorizzazione o la beneficenza a favore di soggetti collegati, e tutte le operazioni che comportino la generazione di una perdita per la Sede Secondaria e la creazione di un utile per i soggetti predetti (es. stralcio ingiustificato di posizione debitoria e/o applicazioni di sconti o condizioni non in linea con i parametri di mercato);
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico; ciò al fine di prevenire il rischio di commissione di reati di "corruzione", nelle loro varie tipologie, di "induzione indebita a dare o promettere utilità" e di "traffico di influenze illecite" che potrebbero derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto con la Sede Secondaria.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

4.7. Gestione della formazione finanziata

4.7.1 Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione della formazione finanziata.
La formazione finanziata è gestita internamente dal Team HR, che si occupa della programmazione e della gestione amministrativa relative alla fruizione dei fondi. La responsabilità di interfacciarsi direttamente con i fondi e gli enti pubblici erogatori di finanziamenti, sovvenzioni o contributi è invece affidata a una società terza, esterna e appositamente incaricata.
Attraverso la gestione della formazione finanziata, la Sede Secondaria, laddove sussistano i presupposti, usufruisce di finanziamenti, sovvenzioni e contributi per la formazione concessi da soggetti pubblici nazionali ed esteri, tra i quali si citano a titolo esemplificativo e non esaustivo:

- **Fondo Sociale Europeo** (finanziamenti alla formazione di occupati/disoccupati – contributi comunitari regionali e provinciali);
- **Fon.Dir.** (fondo paritetico interprofessionale nazionale per la formazione continua dei dirigenti del terziario);
- **FBA** (Fondo Banche e Assicurazioni);

Ai sensi del D. Lgs. n. 231/2001, tali attività potrebbero presentare occasioni per la commissione dei reati di:

- **corruzione** nelle varie tipologie,
- **induzione indebita a dare o promettere utilità**,
- **traffico di influenze illecite**,
- **truffa aggravata per il conseguimento di erogazioni pubbliche**,
- **malversazione a danno dello Stato**,
- **indebita percezione di erogazioni a danno dello Stato**.

Il presente protocollo è finalizzato a garantire il rispetto da parte della Sede Secondaria della normativa vigente e dei principi di **trasparenza, correttezza, oggettività e tracciabilità** nello svolgimento delle attività in oggetto.

4.7.2 Descrizione Del Processo

La gestione della formazione finanziata all'interno della Sede Secondaria è affidata al Team HR, che si occupa di tutte le attività interne connesse alla pianificazione e organizzazione dei corsi. Attualmente non è presente una procedura interna formalizzata, ma la gestione è comunque svolta nel rispetto dei principi di correttezza e tracciabilità.
Il processo prevede:

- Programmazione e organizzazione interna della formazione;
- Raccolta delle adesioni e gestione delle partecipazioni ai corsi da parte del Team HR;
- Raccolta e archiviazione interna degli attestati e della documentazione relativa ai corsi erogati.
- La società terza appositamente incaricata, si occupa:

- della gestione operativa dei bandi e delle pratiche relative alla formazione finanziata;
- della presentazione delle domande di finanziamento e dei rendiconti ai fondi pubblici e agli enti erogatori;
- della gestione dei rapporti con i fondi (es. FBA, FonDir) e con gli enti pubblici o regolatori, in qualità di soggetto esterno delegato.

La Sede Secondaria non gestisce direttamente i rapporti con i fondi o con gli enti pubblici, limitandosi al governo interno delle attività formative e alla supervisione della documentazione prodotta.

4.7.3 Principi Di Controllo

Il sistema di controllo interno a presidio del processo di gestione della formazione finanziata si basa sui seguenti principi:

Livelli autorizzativi definiti
La gestione delle attività connesse alla formazione finanziata è attribuita al **Team HR**, che agisce secondo le responsabilità definite nell'organizzazione interna.

- I referenti HR sono responsabili della raccolta delle adesioni ai corsi e della verifica della regolare partecipazione del personale.
- Le attività di gestione dei bandi e di rendicontazione verso i fondi pubblici e gli enti regolatori sono affidate esclusivamente al soggetto esterno incaricato sulla base di un mandato formalizzato.

Segregazione dei compiti
È garantita una separazione tra:

- le attività interne di raccolta partecipazioni e gestione attestati (a cura del Team HR);
- le attività di interlocuzione con i fondi e gli enti pubblici, la presentazione dei progetti e la gestione dei rendiconti (a cura esclusiva della società terza).

Tracciabilità del processo
Tutta la documentazione relativa alla partecipazione ai corsi (ad esempio, elenchi dei partecipanti, attestati, registri delle presenze) è archiviata dal Team HR, in formato cartaceo e/o elettronico, garantendo così la completa tracciabilità delle attività svolte e delle relative responsabilità.
Le comunicazioni ufficiali con i fondi e gli enti pubblici sono gestite dalla società terza incaricata, che provvede anche all'archiviazione della relativa documentazione, mantenendo copia disponibile al Team HR per eventuali verifiche interne o audit.

Attività di controllo e verifica

Il Team HR assicura:

- la verifica della corrispondenza tra i partecipanti effettivi ai corsi e le dichiarazioni fornite;
- il controllo della completezza e correttezza della documentazione trasmessa alla società terza per le attività di rendicontazione;
- il monitoraggio periodico dell'avanzamento delle attività formative finanziate e dello stato delle pratiche di finanziamento.

Sistema premiante e incentivi

Non sono previsti sistemi di incentivazione collegati alla gestione della formazione finanziata tali da poter determinare comportamenti non coerenti con i principi di correttezza e trasparenza.

4.7.4 Principi di Comportamento

Le Strutture, a qualsiasi titolo coinvolte nella gestione della formazione finanziata, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge vigenti, la normativa interna aziendale nonché le eventuali previsioni del Codice Etico.

In particolare:

- Tutti i soggetti che, in fase di richiesta e gestione dei finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della Sede Secondaria devono essere espressamente autorizzati.
- I soggetti coinvolti nel processo e responsabili della firma di atti o documenti aventi rilevanza esterna (es. pratiche di richiesta, studi di fattibilità, piani di progetto) devono essere appositamente incaricati.
- Il personale non può dare seguito a richieste di indebiti vantaggi o a tentativi di concussione da parte di funzionari pubblici, di cui venga a conoscenza, e deve immediatamente segnalarli al proprio Responsabile, il quale è tenuto a trasmettere la segnalazione alla struttura di Internal Audit per le valutazioni del caso e gli eventuali adempimenti verso l'Organismo di Vigilanza.
- Qualora siano coinvolti soggetti terzi nella predisposizione delle pratiche o nell'esecuzione di attività connesse ai programmi finanziati, i relativi contratti devono contenere una dichiarazione di conoscenza e impegno al rispetto della normativa di cui al D. Lgs. n. 231/2001 e della normativa anticorruzione.
- La corresponsione di onorari o compensi a collaboratori o consulenti esterni è soggetta a preventivo visto da parte dell'unità organizzativa competente, che valuta la qualità della prestazione e la congruità del compenso. Non è consentito riconoscere compensi non giustificati in relazione all'incarico svolto.

È fatto divieto assoluto di porre in essere, collaborare o favorire comportamenti che possano integrare reati ai sensi del D. Lgs. n. 231/2001, in particolare ma non solo:

- Esibire documenti incompleti o comunicare dati falsi o alterati.
- Tenere comportamenti ingannevoli volti a indurre in errore gli Enti finanziatori o erogatori riguardo alla documentazione presentata.
- Chiedere o indurre, anche tramite intermediari, trattamenti di favore da parte della Pubblica Amministrazione o omettere informazioni dovute al fine di influenzare indebitamente le decisioni sulle domande di contributo.
- Destinare contributi, sovvenzioni o finanziamenti pubblici a finalità diverse da quelle per cui sono stati ottenuti.
- Promettere, versare o offrire, anche tramite intermediari, somme di denaro non dovute, doni o vantaggi di qualsiasi natura a soggetti della Pubblica Amministrazione per favorire interessi della Sede Secondaria nell'ottenimento di contributi, inclusi vantaggi impropri quali assunzioni, sponsorizzazioni o donazioni legate a soggetti collegati.
- Affidare incarichi a consulenti esterni eludendo criteri documentabili e oggettivi quali professionalità, competenza, trasparenza, competitività e integrità, in modo da prevenire rischi di corruzione, induzione indebita o traffico di influenze illecite.

I Responsabili delle Strutture coinvolte devono adottare tutte le misure necessarie a garantire l'effettiva applicazione e il rispetto di questi principi di controllo e comportamento.
I principi di cui sopra si estendono, per quanto compatibili, a qualsiasi altro processo aziendale relativo alla richiesta e gestione di contributi o incentivi pubblici concessi alla Sede Secondaria a qualsiasi titolo.

4.8. Gestione dei contenziosi e degli accordi transattivi

4.8.1 Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione dei contenziosi giudiziali e stragiudiziali (amministrativo, civile, penale, fiscale, giuslavoristico e previdenziale) e degli accordi transattivi con Enti pubblici o con soggetti privati.
Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe potenzialmente presentare occasioni per la commissione dei reati di:

- "corruzione", nelle sue varie tipologie,
- "induzione indebita a dare o promettere utilità",
- "traffico di influenze illecite",
- "truffa ai danni dello Stato o di altro ente pubblico",
- "induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria".

Sussiste altresì il rischio della commissione del reato di "corruzione tra privati" e

di “istigazione alla corruzione tra privati”.
Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

4.8.2 Descrizione del Processo

Il processo di gestione del contenzioso si articola nelle seguenti fasi, effettuate sotto la responsabilità delle Strutture competenti per materia, in coordinamento con la Struttura interessata dalla controversia e con gli eventuali professionisti esterni incaricati:

- apertura del contenzioso giudiziale o stragiudiziale;
  - raccolta delle informazioni e della documentazione relative alla vertenza;
  - analisi, valutazione e produzione degli elementi probatori;
  - predisposizione degli scritti difensivi e successive integrazioni, direttamente o in collaborazione con i professionisti esterni;
- gestione della vertenza;
- ricezione, analisi e valutazione degli atti relativi alla vertenza;
- predisposizione dei fascicoli documentali;
- partecipazione, ove utile o necessario, alla causa, in caso di contenzioso giudiziale;
- intrattenimento di rapporti costanti con gli eventuali professionisti incaricati, individuati nell’ambito dell’apposito albo;
- assunzione delle delibere per:
  - determinazione degli stanziamenti al Fondo Rischi e Oneri in relazione alle vertenze passive e segnalazione dell’evento quale rischio operativo;
  - esborsi e transazioni;
  - chiusura della vertenza.

Il processo di gestione degli accordi transattivi riguarda tutte le attività necessarie per prevenire o dirimere una controversia attraverso accordi o reciproche rinunce e concessioni, al fine di evitare l’instaurarsi o il proseguire di procedimenti giudiziari.
Il processo si articola nelle seguenti fasi:

- analisi dell’evento da cui deriva la controversia e verifica dell’esistenza di presupposti per addivenire alla transazione;
- gestione delle trattative finalizzate alla definizione e alla formalizzazione della transazione;
- redazione, stipula ed esecuzione dell’accordo transattivo.

Le modalità operative per la gestione del processo sono disciplinate nell’ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

4.8.3 Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti: la gestione dei contenziosi e degli accordi transattivi, inclusi quelli con la Pubblica Amministrazione prevede l'accentramento delle responsabilità di indirizzo e/o gestione e monitoraggio delle singole fasi del processo in capo a diverse Strutture della Sede Secondaria a seconda che si tratti di profili giuridici di natura amministrativa, civile, penale, fiscale, giuslavoristica e previdenziale. È inoltre previsto nell'ambito di ciascuna fase operativa caratteristica del processo:
  - il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni, nonché le facoltà di autonomia per la gestione del contenzioso ivi incluso quello nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
  - il conferimento degli incarichi a legali esterni diversi da quelli individuati nell'ambito dell'albo predisposto e approvato dalla Struttura competente è autorizzato dal Responsabile della Struttura medesima o da un suo delegato.
- Segregazione dei compiti: attraverso il chiaro e formalizzato conferimento di compiti e responsabilità nell'esercizio delle facoltà assegnate nello svolgimento delle attività di cui alla gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione. In particolare, le procedure aziendali prevedono adeguati livelli quantitativi oltre ai quali le singole transazioni devono essere autorizzate da funzioni diverse da quelle di business che hanno gestito la relazione.
- Attività di controllo:
  - rilevazione e monitoraggio periodico delle vertenze pendenti;
  - verifica periodica della regolarità, della completezza e correttezza di tutti gli adempimenti connessi a vertenze / transazioni che devono essere supportati da meccanismi di *maker* e *checker*.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ciascuna fase rilevante del processo deve risultare da apposita documentazione scritta;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è altresì responsabile dell'archiviazione e della conservazione della documentazione di competenza anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione dei contenziosi e degli accordi transattivi ivi inclusi quelli con la Pubblica Amministrazione.

4.8.4 Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nella gestione dei contenziosi e degli accordi transattivi ivi inclusi quelli con la Pubblica

Amministrazione sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.
In particolare:

- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla Younited devono essere appositamente incaricati;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del contenzioso e degli accordi transattivi, i contratti / lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo è vietato, al fine di favorire indebitamente interessi della Sede Secondaria, ed anche a mezzo di professionisti esterni o soggetti terzi:

- in sede di contatti formali od informali, o nel corso di tutte le fasi del procedimento:
  - avanzare indebite richieste o esercitare pressioni su Giudici o Membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio);
  - indurre chiunque al superamento di vincoli o criticità ai fini della tutela degli interessi della Sede Secondaria;
  - indurre con violenza o minaccia o, alternativamente, con offerta o promessa di denaro o di altra utilità[2], - a tacere o a mentire la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;
  - influenzare indebitamente le decisioni dell'Organo giudicante o le posizioni della Pubblica Amministrazione, quando questa sia controparte del contenzioso/arbitrato;
- in occasione di ispezioni/controlli/verifiche influenzare il giudizio, il parere, il

rapporto o il referto degli Organismi pubblici o nominati dall'Organo giudicante o della Polizia giudiziaria; chiedere o indurre - anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Sede Secondaria;

- promettere versare/offrire - anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), o accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di soggetti della Pubblica Amministrazione, di esponenti apicali
- o persone a loro subordinate appartenenti a società controparti o in relazione con la Sede Secondaria, al fine di favorire indebitamente gli interessi della Sede Secondaria, oppure minacciarli di un danno ingiusto per le medesime motivazioni. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, e tutte le operazioni che comportino la generazione di una perdita per la Younited e la creazione di un utile per i soggetti predetti;
- affidare incarichi a professionisti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del professionista devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico; ciò al fine di prevenire il rischio di commissione del reato di "corruzione" nelle loro varie tipologie, di "induzione indebita a dare o promettere utilità" e di "traffico di influenze illecite" che potrebbero derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare il rapporto con la Sede Secondaria.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

4.9. Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali

4.9.1 Premessa

Il presente protocollo si applica a tutte le strutture della Sede Secondaria coinvolte nella gestione delle procedure acquisitive dei beni e dei servizi.

Tra i beni vanno considerate anche le opere dell'ingegno di carattere creativo, mentre tra le prestazioni vanno ricomprese anche quelli a contenuto intellettuale di qualsiasi natura (es. legale, fiscale, tecnica, giuslavoristica, amministrativa, organizzativa, incarichi di mediazione, d'agenzia o di intermediazioni varie, accordi di collocamento ecc.), ivi incluso il conferimento di incarichi professionali ovvero di consulenze.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "*corruzione*" nelle loro varie tipologie e di "*induzione indebita a dare o promettere utilità",* di *"traffico di*

influenze illecite".
Una gestione non trasparente del processo, infatti, potrebbe consentire la commissione di tali reati, ad esempio attraverso la creazione di fondi "neri" a seguito del pagamento di prezzi superiori all'effettivo valore del bene/servizio ottenuto.
Sussiste altresì il rischio della commissione dei reati di "*corruzione tra privati*" e di "*istigazione alla corruzione tra privati*", descritti nel paragrafo 4.2 nonché i reati *"tributari*", descritti nel paragrafo 6.
Si intende inoltre prevenire il rischio di acquisire beni o servizi di provenienza illecita, ed in particolare il coinvolgimento in altri reati al cui rischio potrebbe essere esposta l'attività della controparte (reati contro l'industria ed il commercio, reati in materia di violazione del diritto d'autore reati di "impiego di clandestini e di intermediazione illecita e sfruttamento del lavoro[3], ecc.). Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

4.9.2 Descrizione del Processo

La gestione degli approvvigionamenti e la scelta dei fornitori seguono un processo formalizzato che coinvolge tutti i Team aziendali con responsabilità in materia di acquisti.

Tutte le richieste di spesa vengono inserite dai Team nel **tool di procurement integrato in Oracle**, a garanzia di tracciabilità e trasparenza.
L'attività di gestione delle procedure per l'acquisizione di beni e servizi si articola nei seguenti processi principali:

- Definizione e gestione del budget;
- Gestione degli approvvigionamenti;
- Gestione del ciclo passivo;
- Gestione dei fornitori.

Le modalità operative per la gestione di tali processi sono disciplinate dalla normativa interna, sviluppata e aggiornata dalle Strutture competenti, che costituisce parte integrante del presente protocollo.

Le spese inserite sono sottoposte al seguente iter approvativo:

- Per importi inferiori a 100.000 euro: l'approvazione è di competenza del Team Finance.
- Per importi pari o superiori a 100.000 euro: l'approvazione è demandata all'Head of Direction.

Al momento della ricezione della fattura:

- viene effettuata una verifica di coerenza tra l'importo fatturato e l'importo precedentemente approvato;
- qualora la fattura presenti uno scostamento superiore al 15% rispetto all'importo approvvigionato, è previsto un passaggio formale con il Team proponente per ottenere l'autorizzazione al pagamento.

I pagamenti sono gestiti direttamente dalla Casa Madre.

Attualmente non è prevista una procedura centralizzata obbligatoria per l'avvio di gare o procedure comparative: tali attività sono gestite autonomamente dai singoli Team in funzione delle specifiche esigenze e della natura dei beni o servizi da acquisire.

4.9.3 Gestione e monitoraggio del budget

Per ciascuna area di approvvigionamento:

- il budget viene definito a inizio esercizio;
- è soggetto ad approvazione del Country Manager e della Casa Madre;
- i team sono tenuti al rigoroso rispetto dei limiti di budget approvati.

4.9.4 Principi di controllo

Il sistema di controllo per garantire la corretta gestione dei processi descritti si basa sui seguenti fattori fondamentali:

Livelli autorizzativi definiti
- **Approvazioni e poteri decisionali:**

L'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà secondo il sistema di poteri e deleghe vigente, che definisce le autonomie gestionali per natura di spesa e impegno. La normativa interna specifica tali meccanismi autorizzativi, indicando i soggetti aziendali titolati a esercitare tali poteri.

- **Scelta dei fornitori:**

La selezione dei fornitori di beni e servizi e dei professionisti avviene tra nominativi selezionati in base a criteri previsti dalla normativa interna, fatte salve esigenze o forniture occasionali. I fornitori, così come eventuali subappaltatori da loro incaricati, devono garantire e, su richiesta, documentare:

- il rispetto della normativa relativa alla proprietà industriale, al diritto d'autore e la legittima provenienza dei beni forniti;
- la conformità alle normative sull'immigrazione e la regolarità retributiva, contributiva, previdenziale, assicurativa e fiscale dei lavoratori impiegati.

- **Subappalto:**

L'eventuale affidamento in subappalto da parte dei fornitori è contrattualmente subordinato al preventivo assenso della struttura della Sede Secondaria che ha stipulato il contratto.

- **Autorizzazione al pagamento:**

L'autorizzazione al pagamento delle fatture spetta ai Responsabili delle Strutture titolari di budget e relativi poteri di spesa (Centri di Responsabilità) o a soggetti delegati. Tale autorizzazione può essere negata a fronte di formale contestazione documentata di inadempienze o carenze nella fornitura. Il pagamento delle fatture è effettuato da una specifica struttura aziendale dedicata.

Segregazione dei compiti

- Le attività delle diverse fasi del processo devono essere svolte da soggetti differenti, chiaramente identificabili, con un meccanismo di **maker-checker** a garanzia della separazione dei compiti.

Attività di controllo

La normativa interna definisce i controlli da svolgere in ogni fase del processo da parte delle Strutture coinvolte, tra cui:

- verifica dei limiti di spesa e della pertinenza della stessa;
- verifica della regolarità, completezza, correttezza e tempestività delle scritture contabili;
- verifica del rispetto dei criteri aziendali per la scelta di fornitori e professionisti, che deve essere preceduta da una adeguata due diligence;
- verifica del rispetto delle norme che vietano o limitano il conferimento di incarichi a dipendenti pubblici o ex dipendenti pubblici.
- Per quanto riguarda incarichi professionali o consulenze che comportano rapporti diretti con la Pubblica Amministrazione (es. spese legali, consulenze per pratiche edilizie o acquisizione di contributi pubblici), i Responsabili delle Strutture devono:
- mantenere aggiornato un elenco di professionisti/consulenti con indicazione di oggetto dell'incarico e corrispettivo;
- effettuare verifiche periodiche dell'elenco per identificare eventuali anomalie.

Tracciabilità del processo

- **Sistemi informativi**: L'operatività deve essere supportata da sistemi informatici che garantiscano la registrazione e archiviazione dei dati e delle informazioni relativi al processo di acquisizione.
- **Documentazione**: Ogni attività deve essere documentata, con particolare attenzione alla fase di individuazione del fornitore o professionista, anche attraverso gare o acquisizione di più offerte. Devono essere motivate la scelta, la pertinenza e la congruità della spesa.
  La normativa interna definisce i casi in cui è obbligatorio procedere con gara o più offerte.
- **Archiviazione e conservazione**: Le strutture responsabili devono garantire l'archiviazione e conservazione, anche in formato elettronico, di tutta la

documentazione prodotta nell'ambito delle procedure di acquisizione, per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate.

a. Criteri per la scelta del fornitore

La selezione dei fornitori si basa su criteri oggettivi, che devono essere documentati e motivati:

- i criteri di scelta vengono formalizzati e tracciati attraverso un business plan predisposto dal Team Finance;
- i Team sono tenuti a rispettare i limiti del budget approvato per la propria area di spesa;
- nel caso in cui una spesa ecceda il budget assegnato, l'approvazione della stessa è sottoposta alla valutazione e all'autorizzazione del CEO.

Il Team General Counsel è responsabile delle verifiche sui fornitori (es. DURC e documentazione obbligatoria).

In conformità alla Politica di Gruppo in materia di esternalizzazione, ogni qualvolta sia prevista l'esternalizzazione di un'attività:

- viene attivato un processo formalizzato di due diligence e controllo cd. processo KYP (Know Your Partner), che comprende:
  - la realizzazione di risk assessment specifici in base alla tipologia di servizio e al fornitore;
  - il rispetto dei passaggi autorizzativi obbligatori previsti dalle procedure di Gruppo.

Oltre alla Procedura di Gruppo, è prevista una procedura interna che impone un processo standardizzato per la selezione e l'onboarding di nuovi provider, articolato in queste fasi:

- identificazione della controparte;
- acquisizione delle evidenze documentali necessarie;
- esecuzione della due diligence tramite la piattaforma Dotfile, che effettua:
  - uno screening digitale dei dati essenziali (es. denominazione sociale, titolare effettivo);
  - lettura automatica dei documenti caricati, con individuazione di eventuali criticità o anomalie;
  - verifiche e confronti dei dati raccolti con fonti esterne per garantirne l'affidabilità;
  - valutazione della reputazione del fornitore.

b. Presidio contrattuale

Il Team Legal cura il presidio contrattuale attraverso i seguenti passaggi:

- sottoscrizione di un NDA (Non-Disclosure Agreement) all'avvio delle interlocuzioni con nuove controparti;
- conduzione di risk assesment mirati;
- supervisione e negoziazione dei contratti sino alla loro finalizzazione;
- sottoscrizione finale dei contratti da parte del Country Manager.

c. Monitoraggio della performance dei fornitori

Il monitoraggio della performance varia in funzione della tipologia di provider:

- Per i fornitori rientranti nel perimetro dell'outsourcing:
  - è obbligatoria la definizione contrattuale di Service Level Agreement (SLA), in linea con la policy di Casa Madre;
  - è previsto un sistema di controllo continuo mediante:
    - verifiche periodiche;
    - comitati periodici che monitorano l'andamento dei servizi e dei contratti;
    - allineamenti mensili e trimestrali;
    - controlli qualitativi specifici (es. nel caso di outsourcing del back office o del customer care).
- Per altre tipologie di provider (non soggette a SLA):
  - è comunque assicurato un controllo continuo mediante verifiche da parte delle funzioni di business responsabili.

4.9.5 Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nel processo di gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.
In particolare:

- la documentazione contrattuale che regola il conferimento di incarichi di fornitura/incarichi professionali deve contenere un'apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;
- i pagamenti devono essere effettuati esclusivamente su un conto corrente intestato al fornitore/ consulente titolare della relazione;
- non è consentito effettuare pagamenti in contanti, né pagamenti in un Paese diverso da quello in cui è insediata la controparte o a un soggetto diverso dalla stessa.

In ogni caso è fatto divieto di porre in essere, collaborare, dare causa alla realizzazione di comportamenti che possano risultare strumentali alla commissione di fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- assegnare incarichi di fornitura ed incarichi professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;

- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori della Younited che non trovino adeguata giustificazione nel contesto del rapporto contrattuale in essere con gli stessi;
- minacciare i fornitori di ritorsioni qualora effettuino prestazioni a favore o utilizzino i servizi di concorrenti della Younited;
- promettere versare/offrire - anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la Sede Secondaria, al fine di favorire indebitamente gli interessi della Younited, oppure minacciarli di un danno ingiusto per le medesime motivazioni. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, e tutte le operazioni che comportino la generazione di una perdita per la Sede Secondaria e la creazione di un utile per i soggetti predetti (es. stralcio ingiustificato di posizione debitoria e/o applicazioni di sconti o condizioni non in linea con i parametri di mercato).

I principi di controllo e di comportamento illustrati nel presente protocollo devono intendersi altresì estesi, per quanto compatibili, all'attività di concessione a terzi (*partner commerciali*) di spazi in locazione per la promozione e vendita di prodotti.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

4.10. Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni

4.10.1 Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni.

Si precisa che, ai fini del presente protocollo, valgono le seguenti definizioni:

- per omaggi si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine della Younited;
- per spese di rappresentanza si intendono le spese sostenute dalla Sede

Secondaria nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Younited (ad es.: spese per colazioni e rinfreschi, spese per forme di accoglienza ed ospitalità, ecc.);
- per iniziative di beneficenza si intendono le elargizioni in denaro che la Sede Secondaria destina esclusivamente ad Enti senza fini di lucro;
- per sponsorizzazioni si intendono la promozione, la valorizzazione ed il potenziamento dell'immagine della Sede Secondaria attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con enti esterni (ad es.: società o gruppi sportivi che svolgono attività anche dilettantistica, Enti senza fini di lucro, Enti territoriali ed organismi locali, ecc.).

Ai sensi del D. Lgs. n. 231/2001, i relativi processi potrebbero costituire una delle modalità strumentali attraverso cui commettere i reati di "*corruzione*", nelle loro varie tipologie, e di "*induzione indebita a dare o promettere utilità*", e di "*traffico di influenze illecite*".
Sussiste altresì il rischio della commissione dei reati di "*corruzione tra privati*" e di "*istigazione alla corruzione tra privati*" descritti nel paragrafo 3. Una gestione non trasparente dei processi relativi a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali, e/o persone loro subordinate o enti, controparti o in relazione con la Sede Secondaria al fine di favorire interessi della Younited ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.
Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

4.10.2 Descrizione del Processo

La gestione delle procedure descritte si inserisce all'interno di un quadro più ampio di regole e strumenti aziendali, che partono da direttive e policy definite a livello di Gruppo e vengono trasposte e adattate all'interno della Sede Secondaria. Tra i principali riferimenti si evidenziano:
- Codice di Condotta
- Codice Etico
- Policy sui Conflitti di Interesse
- Gift & Invitation Policy

In particolare, la Gift & Invitation Policy prevede una soglia di segnalazione per inviti o omaggi ricevuti o offerti. Superata tale soglia, è obbligatorio aprire un ticket e portare la questione all'attenzione del Team Legal per le valutazioni del caso.

4.11. Gestione di omaggi e spese per beneficenze e sponsorizzazioni

La gestione degli omaggi, inviti, sponsorizzazioni e attività di beneficenza è affidata al Team HR ed è disciplinata dalla Gift & Invitation Policy. Tale Policy definisce i criteri e le modalità operative per garantire una gestione corretta e conforme di tali attività, nel rispetto dei principi di trasparenza, integrità e aderenza alla normativa vigente.
I processi di gestione degli omaggi e delle spese di rappresentanza riguardano i beni destinati ad essere offerti, in qualità di cortesia commerciale, a soggetti terzi quali clienti, fornitori, Enti della Pubblica Amministrazione, istituzioni pubbliche o altre organizzazioni.
Si considerano atti di cortesia commerciale e/o istituzionale di modico valore gli omaggi o qualsiasi altra utilità (quali inviti ad eventi sportivi, spettacoli, biglietti omaggio, ecc.) provenienti o destinati allo stesso soggetto o ente, che non superino, nel corso di un anno solare, il valore di 150 euro.

I processi di gestione delle spese per beneficenze e sponsorizzazioni si articolano nelle seguenti fasi:
- individuazione delle società o organizzazioni cui destinare le elargizioni;
- svolgimento delle attività di due diligence da parte della Sede Secondaria;
- esame e valutazione dell'iniziativa o progetto proposto;
- autorizzazione alla spesa e, se previsto, stipula dell'accordo o contratto;
- erogazione delle elargizioni da parte della Sede Secondaria.

Le modalità operative per la gestione di tali processi sono disciplinate da normativa interna, sviluppata e aggiornata dalle Strutture competenti, e costituiscono parte integrante e sostanziale del presente protocollo.

4.11.1 Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

Livelli autorizzativi definiti:

- Per quanto attiene ai beni destinati ad omaggi ed alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere, che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
- Tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
- Gli omaggi o le altre utilità di valore superiore a 150 euro possono essere ammissibili in via eccezionale, in considerazione del profilo del donante o del beneficiario, e comunque nei limiti della ragionevolezza, previa autorizzazione

del Responsabile di livello gerarchico almeno pari a Responsabile di Direzione o struttura aziendale equivalente. I limiti di importo previsti, su base annua per gli omaggi e altre utilità, non si applicano alle spese di rappresentanza relative a colazioni, rinfreschi, eventi e forme di accoglienza e ospitalità che vedano la partecipazione di esponenti aziendali e personale della Sede Secondaria, purché strettamente inerenti al rapporto di affari e ragionevoli rispetto alle prassi di cortesia commerciale e/o istituzionale comunemente accettate;

- Sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.

- Gift & Invitation Policy:
  - La gestione degli omaggi e degli inviti rientra nella Gift e Invitation Policy, la quale prevede una soglia di segnalazione per inviti o omaggi;
  - Qualora il valore di un invito o omaggio superi la soglia stabilita, è obbligatorio aprire un ticket formale e portare la situazione all'attenzione del Team Legal per la valutazione e l'eventuale autorizzazione;
  - Tale procedura assicura la trasparenza e la conformità alle normative interne e alle best practice aziendali.

Segregazione dei compiti: tra i differenti soggetti coinvolti nei processi. In particolare:

- Le attività di cui alle diverse fasi dei processi devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.

Attività di controllo:

- La normativa interna definisce le modalità con le quali le erogazioni relative a beneficenze e sponsorizzazioni devono essere precedute da un'attività di due diligence da parte della Struttura interessata. In particolare, è prevista:
  - L'analisi e la verifica del tipo di organizzazione e della finalità per la quale è costituita;
  - La verifica ed approvazione di tutte le erogazioni da parte del Responsabile della Struttura interessata;
  - La verifica che le erogazioni complessive siano stabilite annualmente e trovino capienza in apposito budget deliberato dagli Organi competenti;
  - Per le sponsorizzazioni, è necessaria una puntuale verifica del corretto adempimento della controprestazione, acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa.
- Obblighi dei Responsabili delle Strutture:
  - Disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi distribuiti, nonché le relative date/occasioni di elargizioni. Tale obbligo non si applica per gli omaggi cosiddetti "marchiati", riportanti cioè il logotipo di Younited (quali biro, oggetti per scrivania, ecc.), nonché l'omaggistica standard predisposta dalla Direzione (ad esempio, in occasione di fine anno);
  - Verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.

Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- Completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione, da parte di tutte le Strutture interessate, di una reportistica sulle erogazioni effettuate e sui contratti stipulati;
- Al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta, anche in via telematica o elettronica, inerente all'esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni.

4.11.2 Principi di comportamento

Premesso che le spese per omaggi sono consentite purché di modico valore e, comunque, tali da non compromettere l'integrità e la reputazione di una delle parti e da non influenzare l'autonomia di giudizio del beneficiario, le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nella gestione di omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico. In particolare:

- la Sede Secondaria può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di Enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici della Younited e nel caso di beneficenze, tali enti non devono avere finalità di lucro;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le "sponsorizzazioni" non possono essere oggetto contemporaneo di erogazione per beneficenza;
- le erogazioni devono essere riconosciute esclusivamente su un conto corrente intestato all'ente beneficiario; non è consentito effettuare pagamenti in contanti, in un Paese diverso da quello dell'ente beneficiario o a un soggetto diverso dallo stesso.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di Enti coinvolti in note vicende giudiziarie, pratiche non rispettose dei diritti umani o contrarie alle norme in tema di vivisezione e di tutela dell'ambiente. Non possono inoltre essere oggetto di erogazioni partiti e movimenti politici e le loro articolazioni organizzative, organizzazioni sindacali e di patronato, club (ad esempio Lions, Rotary, ecc.), associazioni e gruppi ricreativi, scuole private, parificate e/o legalmente riconosciute, salvo

specifiche iniziative connotate da particolare rilievo sociale, culturale o scientifico;

- effettuare elargizioni/omaggi a favore di Enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate contravvenendo a quanto previsto nel presente protocollo;
- promettere o versare/offrire - anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi della Sede Secondaria, anche a seguito di illecite pressioni. Il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore), e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con la Sede Secondaria, a fine di favorire indebitamente gli interessi della Younited;
- dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere nonché le indicazioni geografiche e le denominazioni di origine protette.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

4.12. Gestione del processo di selezione e assunzione del personale

4.12.1 Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione del processo di selezione e assunzione del personale.
Il processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "*corruzione*", nelle loro varie tipologie, di "*induzione indebita a dare o promettere utilità*", di "*traffico di influenze illecite*"[27] nonché dei reati di "*corruzione tra privati*" e di "*istigazione alla corruzione tra privati*" (descritti nel paragrafo 3).
Una gestione non trasparente del processo di selezione e assunzione del personale, potrebbe, infatti, consentire la commissione di tali reati attraverso la

promessa di assunzione verso rappresentanti della Pubblica Amministrazione e/o esponenti apicali, e/o persone loro subordinate di società o enti controparti o in relazione con la Sede Secondaria o soggetti da questi indicati, concessa al fine di influenzarne l'indipendenza di giudizio o di assicurare un qualsivoglia vantaggio per la Sede Secondaria.
Sussiste altresì il rischio della commissione del reato di "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*".
Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Younited, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

4.12.2 Descrizione del Processo

Il processo di selezione e assunzione si articola nelle seguenti fasi:
- Selezione del personale:
  - Analisi e richiesta di nuove assunzioni;
  - Definizione del profilo del candidato;
  - Reclutamento dei candidati;
  - Effettuazione del processo selettivo;
  - Individuazione dei candidati.
- Formalizzazione dell'assunzione;
- Definizione delle politiche di remunerazione.

Il processo è gestito tramite una piattaforma esterna che garantisce la tracciabilità di tutti i passaggi, dalla conservazione dei curricula alla fase di candidatura, in coerenza con quanto dichiarato nella sezione "Lavora con noi" del sito aziendale, dove è indicata la politica di non discriminazione.
Nel corso della selezione:
- Vengono effettuati controlli su casellario giudiziale e carichi pendenti;
- È stato introdotto un check aggiuntivo su DOWJONES per ulteriori verifiche di integrità;
- Durante l'assunzione vengono valutati eventuali conflitti di interesse, sebbene non vi sia una procedura formalizzata: le verifiche vengono effettuate caso per caso;
- Non esiste una procedura dedicata sul rispetto delle pari opportunità e della trasparenza nella selezione; tuttavia, è previsto un sistema di test registrato su piattaforma, con dati che restano tracciati e visionabili.

Resta nelle competenze delle Strutture aziendali specificatamente facoltizzate l'istruttoria relativa alla selezione e assunzione di personale specialistico altamente qualificato o destinato a posizioni di vertice (cosiddetta "assunzione a chiamata").

4.12.3 Principi di controllo

Il sistema di controllo a presidio dei processi di selezione e assunzione del personale si fonda sui seguenti elementi:
Livelli autorizzativi definiti:
- il processo di selezione e assunzione è accentrato in capo alla Struttura

competente, che riceve le richieste formali di nuovo personale da parte delle Strutture interessate e ne valuta la coerenza con il budget disponibile e i piani di sviluppo aziendali;
- l'autorizzazione all'assunzione è concessa esclusivamente da personale espressamente abilitato, in conformità al vigente sistema dei poteri e delle deleghe;
- l'assunzione dei candidati ritenuti idonei e autorizzati all'inserimento è curata dalle Unità Organizzative competenti per la Struttura di riferimento.

Segregazione dei compiti:
- il processo prevede una chiara separazione delle responsabilità tra i soggetti coinvolti; in particolare, l'approvazione finale dell'assunzione è affidata a Strutture diverse da quelle che hanno curato le fasi preliminari della selezione, con modalità proporzionate alla rilevanza della posizione da ricoprire nell'organizzazione.

Attività di controllo:
- durante la selezione, il candidato compila un'apposita modulistica standardizzata, finalizzata a garantire la raccolta omogenea e completa delle informazioni rilevanti;
- l'assunzione deve essere preceduta da un'adeguata attività di due diligence, che comprende le verifiche sul casellario giudiziale, sui carichi pendenti, i controlli su DOWJONES e la valutazione di eventuali conflitti di interesse.

Tracciabilità del processo:
- l'intero processo è tracciato sia a livello documentale sia attraverso i sistemi informativi utilizzati (es. piattaforma esterna);
- la Struttura competente è responsabile della corretta archiviazione e conservazione, anche in formato telematico o elettronico, di tutta la documentazione prodotta nelle varie fasi (ad esempio: curricula, application form, test, contratti di lavoro), così da garantire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate.

4.12.4 Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nella gestione del processo di selezione e assunzione del personale, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché eventualmente le eventuali previsioni del Codice Etico.
In particolare:

- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Struttura avente funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- la selezione deve essere effettuata tra una rosa di candidati, salvo il caso di personale specialistico qualificato, di categorie protette ovvero di figure destinate a posizioni manageriali;

- la valutazione comparativa dei candidati deve essere effettuata sulla base di criteri di competenza, professionalità ed esperienza in relazione al ruolo per il quale avviene l'assunzione.

Qualora il processo di assunzione riguardi:

- personale diversamente abile, il reclutamento dei candidati avverrà nell'ambito delle liste di soggetti appartenenti alle categorie protette, da richiedere al competente Ufficio del Lavoro;
- lavoratori stranieri, il processo dovrà garantire il rispetto delle leggi sull'immigrazione del Paese ove è sita l'unità organizzativa di destinazione e la verifica del possesso, per tutta la durata del rapporto di lavoro, dei permessi di soggiorno, ove prescritti;
- ex dipendenti pubblici, il processo dovrà garantire il rispetto dei divieti di legge.
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- promettere o dare seguito - anche a mezzo di intermediari - a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio alla Sede Secondaria;
- promettere o dare seguito a richieste di assunzioni di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la Sede Secondaria ovvero di soggetti da questi indicati, al fine di favorire indebitamente il perseguimento di interessi della Younited con nocumento della stessa.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

4.13. Gestione dei rapporti con i Regolatorie Autorità Di Vigilanza

4.13.1 Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione dei rapporti con i Regolatori con potere di produzione normativa rilevante per la Sede Secondaria ed il Gruppo e riguarda qualsiasi tipologia di attività posta in essere in occasione di segnalazioni, adempimenti, comunicazioni, richieste, istanze. Rientrano altresì le attività di *advocacy* ovvero pareri/proposte/risposte a consultazioni su normative in corso di elaborazione o in essere.
Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati, di "*corruzione*", nelle loro varie tipologie, di "*induzione indebita a dare o promettere utilità*" e di "*traffico di influenze illecite*".
Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti con:

- tutte le Istituzioni italiane ed estere, inclusi a mero titolo esemplificativo e non esaustivo il Parlamento Italiano e gli enti locali, il Governo, la Banca d'Italia, l'AGCM e il Garante per la protezione dei dati personali, Governi/Parlamenti esteri, Autorità di Regolamentazione in Paesi rilevanti per le attività della Sede Secondaria ed il Gruppo;
- tutte le Istituzioni internazionali e multilaterali, inclusi a mero titolo esemplificativo e non esaustivo le Istituzioni comunitarie (Commissione Europea, Consiglio dell'Unione Europea, Parlamento Europeo), le European Supervisory Authorities ("ESAs"), la Banca Centrale Europea, l'European Data Protection Board ("EDPB"), il Financial Stability Board ("FSB"), la Banca Mondiale ("WB") e il Fondo Monetario Internazionale ("FMI").

4.13.2 Descrizione del Processo

La gestione dei rapporti con le Autorità di regolamentazione e vigilanza si articola secondo un modello organizzativo che prevede un presidio locale affidato alla Sede Secondaria, in costante coordinamento e con flussi informativi continui verso la Capogruppo, al fine di garantire coerenza, allineamento e tempestività nella gestione dei rapporti istituzionali.
In particolare:

- La Sede Secondaria gestisce i rapporti con le Autorità locali, in primis la Banca d'Italia, nel rispetto delle linee guida e delle policy di Gruppo, curando le interlocuzioni ordinarie e fornendo alla Capogruppo un aggiornamento costante sulle attività svolte e sugli sviluppi rilevanti.
- La Capogruppo mantiene il presidio complessivo e strategico dei rapporti con le Autorità di vigilanza, delegando alla Sede Secondaria la gestione operativa e il dialogo diretto con le Autorità locali, salvo i casi di maggiore rilevanza o complessità che richiedono un intervento o un coordinamento centrale.
- Il processo è disciplinato e regolato da un insieme di policy di Gruppo per materia, che prevedono la nomina di referenti locali per ciascun ambito. Tra le principali policy applicabili alla Sede Secondaria si segnalano:

- Policy Antiriciclaggio, con designazione di referenti locali per l'implementazione e il monitoraggio delle attività di compliance;
- Policy Trasparenza di Gruppo, recentemente introdotta per rafforzare l'allineamento normativo e la coerenza con le prassi di Gruppo;
- Policy Distribuzione Assicurativa, che disciplina anche gli obblighi di segnalazione (es. Centrale dei Rischi), gestiti dal team Finance, incaricato della raccolta e trasmissione dei dati mediante database predisposti dalla Capogruppo.
- La gestione operativa con la Banca d'Italia avviene attraverso:
- risposte dirette da parte del Finance Manager per i casi ordinari o privi di criticità;
- confronto e coordinamento con il team Group Compliance per i casi complessi, critici o aventi rilievo per l'intero Gruppo.

Le attività di relazione con i Regolatori, sia dirette sia tramite terzi (consulenti, associazioni di categoria, gruppi di interesse), si articolano nelle seguenti tipologie:

- gestione dei contatti e delle interlocuzioni con le Autorità;
- evasione di richieste specifiche e documenti di consultazione;
- predisposizione e invio di istanze formali, position paper o contributi a consultazioni pubbliche.

La Sede Secondaria, oltre a gestire direttamente le interlocuzioni con le Autorità locali per i temi ordinari e di limitata rilevanza di Gruppo, coinvolge tempestivamente la Capogruppo nei casi aventi rilevanza strategica o potenziale impatto per l'intero Gruppo.
Le modalità operative per la gestione dei rapporti con le Autorità sono disciplinate nella normativa interna.

La gestione dei rapporti con le Autorità di Vigilanza è affidata principalmente alla funzione Legal/Compliance della Succursale italiana. I rapporti con enti regolatori – in particolare Banca d'Italia, Agenzia delle Entrate e il Garante per la protezione dei dati personali sono gestiti su base periodica o a fronte di richieste specifiche. L'operatività è condotta localmente, con coinvolgimento della casa madre nei casi di rilievo per il Gruppo o quando previsto da policy.
Le segnalazioni obbligatorie (es. Centrale dei Rischi, segnalazione di vigilanza) sono gestite dal team Finance. Il presidio è assicurato da policy e procedure, sia di gruppo sia locali, articolate per materia (es. antiriciclaggio, trasparenza, distribuzione assicurativa), che regolano ruoli e modalità di interazione con le Autorità.
Il modello di gestione adottato, basato su governance locale integrata con policy centrali, garantisce presidio sui principali rischi di compliance e un monitoraggio efficace dei rapporti con le Autorità.

4.13.3 Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui

seguenti fattori:

Livelli autorizzativi definiti. In particolare:

- i rapporti con i Regolatori sono intrattenuti dal Responsabile della Struttura di riferimento, da soggetti individuati o autorizzati in base allo specifico ruolo attribuito dal funzionigramma ovvero da soggetti individuati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
- gli atti che impegnano contrattualmente la Sede Secondaria devono essere sottoscritti soltanto da soggetti incaricati.

Segregazione dei compiti tra i differenti soggetti coinvolti nel processo. In particolare, le attività *advocacy* sono svolte da strutture diverse rispetto a quelle direttamente interessate dalla normativa oggetto di analisi.

Attività di controllo:

- controlli di completezza, correttezza ed accuratezza della documentazione trasmessa ai Regolatori da parte della Struttura interessata per le attività di competenza che devono essere supportate da meccanismi di *maker* e *checker*;
- verifica del rispetto dei criteri individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti (l'avvio della relazione deve essere preceduta da un'adeguata *due diligence*).

Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- le fasi principali del processo devono risultare da apposita documentazione scritta;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è altresì responsabile dell'archiviazione e della conservazione della documentazione di competenza anche in via telematica o elettronica, inerente alla gestione dei rapporti con i Regolatori.

4.13.4 Principi di comportamento

Le Strutture della Sede Secondaria a qualsiasi titolo coinvolte nel processo di gestione dei rapporti con i Regolatori sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Sede Secondaria devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un soggetto appartenente ai Regolatori e, più in generale alla Pubblica Amministrazione, di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- il personale deve fornire ai Regolatori informazioni veritiere, corrette, accurate,

aggiornate e non fallaci, avendo cura di differenziare i fatti dalle eventuali opinioni ed evitando di rappresentare le informazioni in modo tale da dare luogo, anche in via potenziale, a confusioni, fraintendimenti o errori da parte degli stessi;

- il personale deve manifestare in modo non equivoco e preliminare ogni conflitto di interessi – attuale o anche solo potenziale – con i Regolatori;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dei rapporti con i Regolatori e, più in generale, con la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a fornitori di servizi eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di fornitori di servizi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- chiedere o indurre - anche a mezzo di intermediari - i rappresentanti dei Regolatori e, più in generale, della Pubblica Amministrazione a trattamenti di favore;
- promettere o versare/offrire - anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – ai rappresentanti dei Regolatori e, più in generale, ai soggetti della Pubblica Amministrazione con la finalità di promuovere o favorire interessi della Younited. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, l'erogazione di servizi a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la Sede Secondaria e la creazione di un utile per i soggetti predetti (es. applicazione di sconti o condizioni non in linea con i parametri di mercato);
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico; ciò al fine di prevenire il rischio di commissione di reati di "corruzione" nelle loro varie tipologie, di "induzione indebita a dare o promettere utilità" e di "traffico di influenze illecite" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate ai Regolatori e, più in generale, alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Sede Secondaria.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli

adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

4.14. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Il sistema dei flussi informativi verso l'Organismo di Vigilanza (OdV) è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.
- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua:
  - **verifiche semestrali** sui flussi informativi ricevuti, al fine di monitorare con continuità l'efficacia del Modello 231 e l'adeguatezza delle misure adottate;
  - **una verifica annuale complessiva**, nell'ambito della quale analizza i flussi informativi dell'anno, valuta l'efficacia del sistema dei controlli e propone eventuali azioni correttive o migliorative.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Legal / Finance	- Elenco degli omaggi e/o atti di liberalità elargiti a favore di Enti Pubblici, Pubblici Ufficiali o Incaricati di Pubblico Servizio - Elenco degli omaggi e atti di liberalità ricevuti da Esponenti Aziendali, Dipendenti e/o Consulenti - Elenco degli omaggi o atti di liberalità elargiti nei confronti del medesimo Ente Pubblico, Pubblico Ufficiale o Incaricato di Pubblico Servizio - Elenco dei contratti stipulati con controparti pubbliche, con indicazione della procedura di aggiudicazione delle medesime. - Elenco e copia delle deleghe e procure rilasciate a Esponenti Aziendali, Dipendenti e/o Consulenti al fine di intrattenere rapporti con la Pubblica	Annuale

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
	Amministrazione. - Elenco delle ispezioni ricevute e/o in corso (PA procedente, soggetti partecipanti, periodo di svolgimento). - Trasmissione dei verbali d'ispezione che diano evidenza di criticità. - Elenco dei contenziosi giudiziali in corso e breve descrizione dello status.	
HR	- Elenco delle richieste di finanziamenti, contributi o altre forme di erogazione pubblica. - Rendiconto delle attività svolte per la richiesta di erogazioni pubbliche e dell'impiego di eventuali erogazioni già conseguite.	Annuale
HR	- Reporting sulle attività svolte e volte all'acquisizione di nuovi Consulenti e Fornitori, con indicazione della modalità di assegnazione, accertamento requisiti di onorabilità/professionalità, apposizione di clausole 231 nei contratti.	Semestrale
Organismo di Vigilanza (OdV)	- Verifica delle comunicazioni ricevute (ad hoc su eventi rilevanti). - Pianificazione e realizzazione di interventi di verifica su base semestrale. - Verifica annuale complessiva sui flussi informativi e sull'efficacia complessiva del Modello 231. - Produzione di report periodici sull'attività di vigilanza svolta e sulle risultanze dei controlli effettuati.	Semestrale / Annuale

5. REATI CONTRO L'INDUSTRIA ED IL COMMERCIO ED I REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

5.1. Premessa

La presente Parte Speciale ha l'obiettivo di illustrare i criteri, i ruoli e le responsabilità, i principi di controllo e le regole di comportamento cui tutti i Destinatari, ivi compresi i Consulenti, il personale, i fornitori e i partner, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dall'articolo 25-*bis* 1 del Decreto e dell'art. 10 della l. 146/2006, nel rispetto dei principi di legalità, correttezza, oggettività, trasparenza, tracciabilità e riservatezza nell'esecuzione delle proprie attività, della normativa emanata dagli organismi di vigilanza e di tutte le leggi e gli standard nazionali ed

internazionali vigenti.

5.2. Le fattispecie di reato previste dall'articolo 25-*bis* e 25-*bis* 1 del Decreto e dell'art. 10 della l. 146/2006

La L. 23.7.2009 n. 99 – Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in tema di energia – in un più ampio quadro di iniziative di rilancio dell'economia e di tutela del "*Made in Italy*", dei consumatori e della concorrenza, ha attratto nell'ambito della responsabilità da reato degli Enti numerose norme penali, alcune delle quali dalla stessa legge emanate o riformulate. In particolare, nel testo novellato del D. Lgs. n. 231/2001, gli artt. 25-bis e 25-bis.1 richiamano fattispecie previste dal codice penale in tema di industria e di commercio, mentre l'art. 25-novies - al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno e i gravi danni economici arrecati agli autori e all'industria connessa – rimanda a reati contemplati dalla legge sul diritto d'autore (L. n. 633/1941). Si descrivono qui di seguito gli illeciti in questione.

REATI IN TEMA DI FALSITA' NEI SEGNI DI RICONOSCIMENTO
La nuova disposizione di cui all'articolo 25-*bis* del Decreto 231 ha ampliato la categoria dei reati-presupposto della responsabilità amministrativa dell'ente includendovi le fattispecie di contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti modelli e disegni e prevedendo, in relazione alla commissione di tali reati, l'applicabilità all'ente medesimo di una sanzione pecuniaria fino a 500 (cinquecento) quote.

A fronte della commissione di tali reati, pertanto, le sanzioni pecuniarie possono superare l'importo di euro 750.000,00.
Per i medesimi reati sono previste altresì sanzioni di tipo interdittivo per una durata non superiore a un anno.
Ove l'ente sia responsabile in relazione ad una pluralità di illeciti commessi con un'unica azione od omissione ovvero commessi nello svolgimento di una medesima attività, infine, la sanzione prevista dall'articolo 25-*bis* potrà essere aumentata fino al triplo.
I reati presupposto dell'articolo 25-*bis* riguardano, oltre ai reati in materia di strumenti e segni di riconoscimento sopra descritti, i reati di falsità in monete, in carte di pubblico credito e in valori di bollo.
Tra i reati previsti dall'articolo 25-*bis* si evidenziano i seguenti:

Contraffazione, alterazione o uso di marchi o di segni distintivi ovvero di brevetti, modelli e disegni di prodotti industriali (art. 473 c.p.)
La norma punisce le condotte di chi, pur potendo accertare l'altrui appartenenza di marchi e di altri segni distintivi di prodotti industriali, ne compie la contraffazione, o altera gli originali, ovvero fa uso dei marchi falsi senza aver partecipato alla falsificazione.
Integrano la contraffazione le ipotesi consistenti nella riproduzione identica o nell'imitazione degli elementi essenziali del segno identificativo, in modo tale che ad una prima percezione possa apparire autentico. Si tratta di quelle falsificazioni materiali idonee a ledere la pubblica fiducia circa la provenienza di prodotti o servizi dall'impresa che è titolare, licenziataria o cessionaria del

marchio registrato. Secondo la giurisprudenza è tutelato anche il marchio non ancora registrato, per il quale sia già stata presentata la relativa domanda, in quanto essa lo rende formalmente conoscibile. È richiesto il dolo, che potrebbe sussistere anche qualora il soggetto agente, pur non essendo certo dell'esistenza di altrui registrazioni (o domande di registrazione), possa dubitarne e ciononostante non proceda a verifiche.
Il secondo comma sanziona le condotte di contraffazione, nonché di uso da parte di chi non ha partecipato alla falsificazione, di brevetti, disegni e modelli industriali altrui. Anche questa disposizione intende contrastare i falsi materiali che, nella fattispecie, potrebbero colpire i documenti comprovanti la concessione dei brevetti o le registrazioni dei modelli. La violazione dei diritti di esclusivo sfruttamento economico del brevetto è invece sanzionata dall'art. 517-ter c.p.

Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)
L'art. 474 c.p. punisce le condotte di coloro che, estranei ai reati di cui all'art. 473 c.p., introducono in Italia prodotti industriali recanti marchi o segni distintivi contraffatti o alterati, oppure detengono per la vendita, mettono in vendita o comunque in circolazione prodotti contraffatti, sempre che non siano già punibili per l'introduzione in Italia. È sempre richiesto il fine di trarre profitto.
Il detentore potrebbe essere punito, oltre che per il reato in questione, anche a titolo di ricettazione, qualora fosse a conoscenza fin dal momento dell'acquisto della falsità dei segni distintivi apposti ai prodotti dal suo fornitore o da altri. Si ricorda che, ai sensi dell'art. 25-octies del Decreto, anche il reato di ricettazione può dar luogo alla responsabilità amministrativa degli Enti.

DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

La *ratio* sottesa a queste norme è la persecuzione della disonestà commerciale poiché questo tipo di condotte assicurano un vantaggio competitivo all'imprenditore che le pone in essere danneggiando quindi i suoi competitor e, in ultima analisi, l'intero sistema degli scambi commerciali.
Con particolare riferimento alla frode in commercio, la condotta incriminata si basa sulla consegna di una cosa mobile, consegna che può avvenire non solo nell'ambito del contratto di compravendita, ma anche in relazione ad altri tipi di accordo, come per esempio la permuta, purché si produca l'obbligo di consegna della merce.
Oggetto dello scambio può essere una qualsiasi cosa mobile, la quale possa concretamente essere fatta oggetto di relazioni commerciali, ma non il danaro costituente il prezzo della *res* ceduta, nemmeno i diritti sui beni immateriali, le prestazioni personali e quelle meccaniche, a meno che l'apparecchio meccanico costituisca il tramite per la consegna del bene, come per esempio il distributore automatico.
I potenziali soggetti attivi, rientrando i reati *de quibus* nella categoria dei reati comuni, non sono solo gli imprenditori ma anche i loro collaboratori. In particolare, la responsabilità dei singoli preposti è configurabile nelle aziende di notevoli dimensioni, purché vi sia una suddivisione di attribuzioni con assegnazione di compiti esclusivamente personali a determinati soggetti. Di contro, si ribadisce, in mancanza della assegnazione di specifici compiti a

determinati soggetti, i titolari (amministratori o legali rappresentanti) sono da considerarsi i responsabili del reato di frode in commercio, essendo tenuti ad osservare e far osservare tutte le disposizioni
imperative concernenti gli aspetti dell'attività aziendale.

Turbata libertà dell'industria e del commercio (art. 513 c.p.)
Il reato, perseguibile a querela, consiste nel compiere atti di violenza sulle cose o nell'utilizzare mezzi fraudolenti al fine di ostacolare od impedire il regolare svolgimento di un'attività commerciale od industriale, sempre che non siano integrati reati più gravi (ad es. incendio, oppure uno dei reati informatici previsti dall'art. 24-bis del Decreto). Ad esempio, si è ritenuto sussistere il reato nel caso di inserimento nel codice sorgente del proprio sito internet - in modo da renderlo maggiormente visibile ai motori di ricerca
- di parole chiave riferibili all'impresa o ai prodotti del concorrente, al fine di dirottare i suoi potenziali clienti.

Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.) Commette questo delitto l'imprenditore che compie atti di concorrenza con violenza o minaccia. La norma, introdotta nel codice penale dalla legge antimafia "Rognoni – La Torre" n. 646/1982, trova applicazione anche al di fuori della criminalità mafiosa ed intende contrastare gli atti diretti a impedire o limitare l'intervento sul mercato di operatori concorrenti. Il reato sussiste anche quando la violenza o la minaccia sia posta in essere da terzi per conto dell'imprenditore, oppure non sia direttamente rivolta al concorrente, ma ai suoi potenziali clienti. Potrebbe ad esempio ravvisarsi il reato nelle ipotesi di: minaccia di arrecare un danno ingiusto diretta ai partecipanti a una gara pubblica al fine di conoscere le loro offerte e formularne più basse; minaccia, nel rapporto con un proprio cliente, di applicare condizioni peggiorative o di revocare i crediti concessi, ovvero, nel rapporto con un proprio fornitore, di non effettuare altri ordini nel caso in cui il cliente/fornitore ricorra ai servizi di/fornisca un determinato concorrente.

Frodi contro le industrie nazionali (art. 514 c.p.)
Il delitto incrimina chiunque cagioni un danno contro l'industria nazionale, ponendo in circolazione od in commercio prodotti industriali con marchi o segni distintivi contraffatti. Le dimensioni del danno devono essere tali da colpire non singole imprese, ma l'economia industriale italiana.

Frode nell'esercizio del commercio (art. 515 c.p.)
L'illecito, sempre che non sussistano gli estremi della truffa, consiste nella consegna all'acquirente da parte di chi esercita un'attività commerciale di una cosa mobile per un'altra, o che, pur essendo della stessa specie, per origine, provenienza, qualità o quantità, sia diversa da quella pattuita.

Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
Il reato è commesso di chi pone in vendita o in commercio sostanze alimentari non genuine, vale a dire sostanze, cibi e bevande che, pur non pericolosi per la salute, siano stati alterati con aggiunta o sottrazione di elementi, od abbiano composizione diversa da quella prescritta.

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
Il delitto consiste nel mettere in vendita o comunque in circolazione opere dell'ingegno o prodotti industriali con nomi, marchi o segni distintivi[4] atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto. È sufficiente che i segni distintivi, anche in relazione alle altre circostanze del caso concreto (prezzi dei prodotti, loro caratteristiche, modalità della vendita) possano ingenerare nel comune consumatore confusione con i prodotti affini (ma diversi per origine, provenienza o qualità) contrassegnati dal marchio genuino. La norma tutela l'onestà nel commercio e si applica sussidiariamente, quando non ricorrano gli estremi delle più gravi incriminazioni degli artt. 473 e 474 c.p. In essa ricadono casi quali la contraffazione e l'utilizzo di marchi non registrati, l'uso di recipienti o di confezioni con marchi originali, ma contenenti prodotti diversi, l'uso da parte del legittimo titolare del proprio marchio per contraddistinguere prodotti con standard qualitativi diversi da quelli originariamente contrassegnati dal marchio (il caso non ricorre se la produzione sia commissionata ad altra azienda, ma il committente controlli il rispetto delle proprie specifiche qualitative).

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)
Il reato consta di due diverse fattispecie. La prima, perseguibile a querela, punisce chiunque, potendo conoscere dell'esistenza di brevetti o di registrazioni altrui, fabbrica o utilizza ai fini della produzione industriale oggetti o altri beni, usurpando un titolo di proprietà industriale o in violazione dello stesso. Qualora sussista la falsificazione dei marchi o un'altra delle condotte previste dagli artt. 473 e 474 c.p., l'usurpatore potrebbe rispondere anche di tali reati.
La seconda fattispecie concerne la condotta di chi, al fine di trarne profitto, introduce in Italia, detiene per la vendita, pone in vendita o mette comunque in circolazione beni fabbricati in violazione dei titoli di proprietà industriale. Se le merci sono contraddistinte da segni falsificati si applica anche l'art. 474, comma 2, c.p.
Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)
Le condotte punite consistono nell'apporre a prodotti agroalimentari false o alterate indicazioni geografiche o denominazioni d'origine[5] nonché, ai fini di trarne profitto, nell'introdurre in Italia, detenere per la vendita, porre in vendita o mettere comunque in circolazione i medesimi prodotti con indicazioni o denominazioni contraffatte.
Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941)
Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941)
Commette il primo delitto in esame chiunque, senza averne il diritto, a qualsiasi scopo ed in qualsiasi forma, mette a disposizione del pubblico un'opera dell'ingegno protetta o parte di essa, immettendola in un sistema di reti telematiche mediante connessioni di qualsiasi genere. In alcuni particolari casi - per finalità culturali o di libera espressione ed informazione e con determinate

limitazioni - è consentita la comunicazione al pubblico di opere altrui[6].
Il secondo delitto in oggetto consiste nell'abusivo utilizzo dell'opera dell'ingegno altrui (mediante riproduzione, trascrizione, diffusione in qualsiasi forma, commercializzazione, immissione in reti telematiche, rappresentazione o esecuzione in pubblico, elaborazioni creative, quali le traduzioni, i compendi, ecc.) aggravato dalla lesione dei diritti morali dell'autore. Alla condotta di per sé già abusiva deve cioè aggiungersi anche la violazione del divieto di pubblicazione imposto dall'autore, o l'usurpazione della paternità dell'opera (c.d. plagio), ovvero la sua deformazione, mutilazione, o altra modificazione che offenda l'onore o la reputazione dell'autore.
Entrambe le incriminazioni si applicano in via residuale, quando non risulti presente il dolo specifico del fine di trarre un profitto od un lucro, che deve invece caratterizzare le condotte, in parte identiche, più severamente sanzionate dagli artt. 171-bis e 171-ter.

Abusi concernenti il *software* e le banche dati (art. 171-bis L. n. 633/1941)

Il primo comma della norma, con riferimento ai programmi per elaboratore[7], punisce le condotte di abusiva duplicazione, nonché di importazione, distribuzione, vendita, detenzione a scopo commerciale od imprenditoriale (quindi anche per uso limitato all'ambito della propria impresa), concessione in locazione, quando hanno per oggetto programmi contenuti in supporti privi del contrassegno della Società italiana degli autori ed editori (SIAE). Costituiscono inoltre reato l'approntamento, la detenzione o il traffico di qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione da utilizzi abusivi dei programmi.
Il secondo comma, con riferimento alla tutela dei diritti dell'autore di una banca di dati[8], punisce la riproduzione - permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma - su supporti non contrassegnati dalla SIAE, il trasferimento su altro supporto, la distribuzione, la comunicazione, la presentazione o la dimostrazione in pubblico non autorizzate dal titolare del diritto d'autore. Sono altresì sanzionate le condotte di estrazione e di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati, in violazione del divieto imposto dal costitutore[9] della medesima banca dati. Per estrazione deve intendersi il trasferimento di dati permanente o temporaneo su un altro supporto con qualsiasi mezzo o in qualsivoglia forma e per reimpiego qualsivoglia forma di messa a disposizione del pubblico dei dati mediante distribuzione di copie, noleggio, trasmissione con qualsiasi mezzo e in qualsiasi forma.
Tutte le predette condotte devono essere caratterizzate dal dolo specifico del fine di trarne profitto, vale a dire di conseguire un vantaggio, che può consistere anche solo in un risparmio di spesa.

Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941)

La norma elenca una nutrita casistica di condotte illecite - se commesse per uso non personale e col fine di lucro - aventi ad oggetto: opere destinate al circuito televisivo, cinematografico, della vendita o del noleggio; supporti di qualunque tipo contenenti opere musicali, cinematografiche, audiovisive, loro fonogrammi,

videogrammi o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche, didattiche, musicali, multimediali. Sono infatti punite:

- le condotte di abusiva integrale o parziale duplicazione, riproduzione, diffusione in pubblico con qualsiasi procedimento;
- le condotte, poste in essere da chi non ha partecipato all'abusiva duplicazione o riproduzione, di introduzione in Italia, detenzione per la vendita o distribuzione, messa in commercio, cessione a qualsiasi titolo, proiezione in pubblico o trasmissione televisiva o radiofonica, far ascoltare in pubblico le duplicazioni o riproduzioni abusive;
- le medesime condotte elencate al punto che precede (salvo l'introduzione in Italia e il far ascoltare in pubblico) riferite a supporti di qualunque tipo, anche se non frutto di abusiva duplicazione o riproduzione, privi del prescritto contrassegno SIAE o con contrassegno falso.

Sono altresì sanzionate le condotte abusive concernenti, in sintesi: la diffusione di servizi ricevuti con decodificatori di trasmissioni criptate; i traffici di dispositivi che consentano l'accesso abusivo a detti servizi o di prodotti diretti ad eludere le misure tecnologiche di contrasto agli utilizzi abusivi delle opere protette; la rimozione o l'alterazione delle informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti, ovvero l'importazione o la messa in circolazione di opere dalle quali siano state rimosse od alterate le predette informazioni.

Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941)

Commettono il reato i produttori od importatori di supporti contenenti software destinati al commercio che omettono di comunicare alla SIAE i dati necessari all'identificazione dei supporti per i quali vogliano avvalersi dell'esenzione dall'obbligo di apposizione del contrassegno SIAE[10].

È altresì punita la falsa attestazione di assolvimento degli obblighi di legge rilasciata alla SIAE per l'ottenimento dei contrassegni da apporre ai supporti contenenti software od opere audiovisive.

Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941)

Il delitto è commesso da chiunque, per fini fraudolenti produce, importa, promuove, installa, pone in vendita, modifica o utilizza anche per solo uso personale, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

5.3. Le Attività Aziendali sensibili

Con riferimento all'operatività di gestione del risparmio, i rischi di commissione dei reati contro l'industria ed il commercio ed in materia di violazione del diritto d'autore più verosimilmente possono presentarsi:

- nei rapporti con la clientela, con riguardo alla prestazione di servizi a favore di soggetti coinvolti nelle attività illecite in questione;
- nella partecipazione a gare pubbliche, con particolare riferimento a comportamenti illeciti nei confronti dei partecipanti;
- nell'approvvigionamento o nell'utilizzo di prodotti, software, banche dati ed altre opere dell'ingegno, strumentali all'attività della Sede Secondaria destinati ad omaggi per la clientela;
- nella concessione a terzi (partner commerciali) di spazi fisici e digitali per la promozione e vendita di prodotti e servizi.
- Inoltre, la Società adotta specifici presìdi di controllo e procedure operative, anche in conformità alla normativa di settore, al fine di prevenire e contrastare i rischi connessi alle seguenti attività: ideazione e lancio di nuovi prodotti, gestione del naming e dei marchi del Gruppo, comunicazione esterna e pubblicitaria, iniziative di marketing e gestione dei rapporti con la clientela. Tali misure sono finalizzate a garantire il rispetto dei principi di lealtà della concorrenza, nonché di correttezza e trasparenza delle pratiche commerciali, in linea con i valori etici e comportamentali della Società.

5.4. Descrizione del Processo

La Società, in coerenza con i principi di correttezza, trasparenza e tutela dei consumatori, ha definito una serie di controlli e procedure a presidio del rischio di commissione di reati contro l'industria e il commercio, con particolare riferimento alle attività di marketing e comunicazione commerciale, come previsti dall'art. 25-bis.1 del D.Lgs. 231/2001.

Processo operativo in ambito marketing
In particolare, tutti i materiali di comunicazione destinati al pubblico (online e offline) sono sottoposti a un processo di validazione interna, che garantisce il rispetto delle normative di settore (tra cui il Codice del Consumo, la normativa bancaria e finanziaria e le disposizioni in tema di trasparenza e correttezza dell'informazione pubblicitaria).
Procedura di selezione e gestione dei partner commerciali

- Ogni collaborazione con soggetti terzi (partner marketing) è preceduta da una call di verifica sull'idoneità e sulla pertinenza dell'attività proposta rispetto al target desiderato.
- A seguire, il partner viene valutato dal team legale, anche mediante analisi finanziaria, ed eventualmente approvato per la stipula contrattuale.

- Per tutti i partner è prevista una procedura di onboarding seguendo la procedura KYP (Know Your Partner).

Validazione dei contenuti marketing

- Il materiale promozionale è fornito esclusivamente dalla Società.
- È vietato per i partner pubblicare o inviare materiale marketing non preventivamente approvato dalla Società.
- La procedura operativa prevede che:
  - Il partner invii una preview del materiale da utilizzare;
  - La preview venga esaminata e validata dall'ufficio marketing (composto da 7 risorse, ciascuna assegnata a uno specifico canale);
  - Solo dopo approvazione è autorizzata la pubblicazione o la distribuzione.

Monitoraggio delle performance e gestione del rischio reputazionale

- Su base mensile, in particolare per le campagne e-mail, viene effettuato un monitoraggio della qualità dei lead acquisiti da ciascun partner (es. percentuale di compilazioni errate o con dati non veritieri).
- In presenza di criticità, il partner viene informato e invitato a correggere le anomalie; nei casi più gravi la collaborazione viene interrotta.
- Questo tipo di analisi è eseguito solo sui canali esterni e di terze parti, mentre non è tecnicamente applicabile a canali gestiti da piattaforme pubblicitarie (es. Google Ads).

Prospettive di formalizzazione

È in corso di pubblicazione a livello di Gruppo una nuova policy sulla trasparenza e il layout del marketing, che conterrà anche formalizzazione delle procedure sopra descritte, rafforzando ulteriormente il presidio organizzativo contro i rischi di:

- Comunicazioni commerciali ingannevoli;
- Utilizzo scorretto dei marchi o segni distintivi;
- Promozione non conforme dei prodotti finanziari.

Processo operativo in ambito di approvvigionamento e utilizzo di prodotti, software, banche dati ed altre opere dell'ingegno, strumentali all'attività della Sede Secondaria

In relazione all'approvvigionamento o all'utilizzo di prodotti, software, banche dati, si evidenzia che la gestione delle licenze d'uso è centralizzata a livello di Capogruppo. In particolare:

- Le richieste di nuovi strumenti digitali (es. software, banche dati, applicativi) sono inoltrate tramite apertura di un ticket sull'apposito portale interno;

- L'acquisto e l'attivazione delle licenze è effettuato direttamente dal dipartimento centrale competente, nel rispetto delle condizioni contrattuali e dei diritti di utilizzo previsti dai fornitori;
- La Sede Secondaria non effettua acquisizioni autonome di tali strumenti e si attiene esclusivamente a quanto autorizzato e distribuito dalla casa madre.

Questo processo centralizzato costituisce un presidio di controllo volto a prevenire:

- L'utilizzo non autorizzato o illegittimo di opere protette da diritto d'autore;
- La diffusione di contenuti privi di licenza o acquisiti tramite canali non conformi;
- Il rischio di responsabilità della Società per violazioni in materia di proprietà intellettuale, anche rilevanti ai sensi dell'art. 25-bis.1 del D.Lgs. 231/2001 e dell'art. 10 della L. 146/2006.

5.5. Principi di controllo

Si rimanda ai protocolli già previsti nel presente Modello, che disciplinano ambiti connessi alle attività a rischio e che contengono processi, principi di controllo e regole di condotta idonei a prevenire anche i reati oggetto del presente Capitolo:

- al **paragrafo 7.4**, relativo al *"Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose"*;
- al **paragrafo 4.9**, relativo alla *"Gestione delle procedure acquisitive dei beni, dei servizi e degli incarichi professionali"*;
- al **paragrafo 4.10**, relativo alla *"Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni"*;
- al **paragrafo 11.4**, relativo alla *"Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale"*;
- al **paragrafo 4.5**, relativo alla *"Stipula dei rapporti contrattuali con la Pubblica Amministrazione"*.

Tali protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di specifici contratti di servizio, da parte delle altre sedi del Gruppo e/o da soggetti esterni in outsourcing.
Sebbene dopo il 2022 non siano state introdotte nuove fattispecie di reato nel novero dei reati presupposto di cui all'art. 25-bis.1 del D.Lgs. 231/2001 (Reati contro l'industria e il commercio) e all'art. 10 della Legge 146/2006 (Reati transnazionali, inclusi i reati in materia di diritto d'autore), si segnalano rilevanti evoluzioni normative e giurisprudenziali che impongono un rafforzamento del sistema di controllo preventivo.
In particolare, l'entrata in vigore del D.Lgs. 24/2023 in materia di whistleblowing ha rafforzato l'importanza della segnalazione tempestiva di illeciti, inclusi quelli riguardanti la concorrenza sleale, la contraffazione di prodotti, la violazione di DOP/IGP e le frodi commerciali.
Sul fronte del diritto d'autore, l'attuazione della Direttiva UE 2019/790 (cd. Copyright Directive) ha ridefinito le responsabilità delle piattaforme digitali nella

diffusione di contenuti protetti, aumentando il rischio di coinvolgimento delle persone giuridiche in condotte illecite con valenza transnazionale. Alla luce di tali evoluzioni, il presente Modello è stato aggiornato per includere misure di prevenzione rafforzate in ambito e-commerce, distribuzione digitale e gestione dei diritti di proprietà industriale e intellettuale, anche in un'ottica di cooperazione interstatale e di conformità ai nuovi obblighi europei.

5.6. CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei Destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei principi procedurali ivi previsti ovvero dei principi contenuti nella policy aziendale adottata ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

5.7. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.
- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua verifiche semestrali, annuali e ad evento.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	**Descrizione del flusso informativo**	**Periodicità**
Marketing	Invio policy aggiornate su trasparenza e conformità dei contenuti pubblicitari	Ad evento
Marketing	Comunicazione iniziative promozionali di particolare impatto o rischio (es. campagne nazionali)	Ad evento
Marketing	**Report semestrale**: Report sintetico su attività di marketing, naming e pubblicità, incluse eventuali non conformità rilevate	Semestrale
IT / Acquisti	Informazioni su approvvigionamento e utilizzo di prodotti, software, banche dati e opere dell'ingegno soggetti a licenza	Ad evento
IT / Acquisti	informazione o anomalia relativa a utilizzi non autorizzati	Ad evento

In relazione all'approvvigionamento o all'utilizzo di prodotti, software, banche dati e altre opere dell'ingegno funzionali alle attività della Sede Secondaria, si evidenzia che la **gestione delle licenze d'uso è centralizzata a livello di Capogruppo**. Tuttavia, la Sede Secondaria è tenuta a trasmettere all'OdV ogni informazione o anomalia relativa a utilizzi non autorizzati, richieste di nuovi strumenti digitali, modifiche ai contratti di fornitura o criticità segnalate dai fornitori, in ottica di prevenzione di possibili violazioni del **diritto d'autore e delle norme sulla proprietà intellettuale** (art. 25-novies D.Lgs. 231/2001).

6. REATI TRIBUTARI

6.1. Premessa

La presente Parte Speciale ha l'obiettivo di illustrare i criteri, i ruoli e le responsabilità, i principi di controllo e le regole di comportamento cui tutti i Destinatari, ivi compresi i Consulenti, il personale, i fornitori e i partner, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dall'articolo 25-quinquiesdecies del Decreto e dell'art. 10 della l. 146/2006, nel rispetto dei principi di legalità, correttezza, oggettività,

trasparenza, tracciabilità e riservatezza nell'esecuzione delle proprie attività, della normativa emanata dagli organismi di vigilanza e di tutte le leggi e gli standard nazionali ed internazionali vigenti.

Le fattispecie di reato di cui all'art. 25-*quinquiesdecies* del Decreto

L'art. 25-quinquiesdecies del D.Lgs. 231/2001 ha introdotto nel perimetro dei reati presupposto i delitti tributari, in particolare quelli previsti dal D.Lgs. 74/2000. Tali reati risultano rilevanti qualora commessi da soggetti apicali o sottoposti, nell'interesse o vantaggio dell'Ente.

Tra i reati più rilevanti si annoverano:

- la dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. 74/2000),
- la dichiarazione fraudolenta mediante altri artifici (art. 3),
- la dichiarazione infedele (art. 4),
- l'omessa dichiarazione (art. 5),
- l'emissione di fatture per operazioni inesistenti (art. 8),
- l'indebita compensazione (art. 10-quater),
- la sottrazione fraudolenta al pagamento di imposte (art. 11), nonché i reati connessi alla documentazione contabile e alla corretta rappresentazione fiscale delle operazioni.

Si descrivono qui di seguito gli illeciti in questione.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 d.lgs. 74/2000) La fattispecie punisce chi presenta dichiarazioni relative alle imposte sui redditi o all'IVA che indichino elementi passivi fittizi, risultanti da fatture o da altri documenti registrati nelle scritture contabili obbligatorie o conservati a fini di prova. Le fatture o i documenti utilizzati sono connotati da falsità materiale o ideologica circa l'esistenza in tutto o in parte delle operazioni in essi indicati, o circa il soggetto controparte.

Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. n. 74/2000) Il reato sussiste allorché, al di fuori del caso di uso di fatture o documenti attestanti operazioni inesistenti che precede, in una delle predette dichiarazioni siano indicati elementi attivi inferiori a quelli effettivi, oppure fittizi elementi passivi, crediti e ritenute, mediante la conclusione di operazioni simulate, oggettivamente o soggettivamente, oppure avvalendosi di documenti falsi, registrati nelle scritture contabili obbligatorie o conservati ai fini di prova, o di altri mezzi fraudolenti idonei a falsare la contabilità ostacolando l'accertamento o inducendo in errore l'Agenzia delle Entrate. Tale reato non sussiste quando non sono superate determinate soglie, oppure la falsa

rappresentazione della realtà non sia ottenuto con artifici, ma si tratti di mera omissione degli obblighi di fatturazione e annotazione o della sola indicazione in dichiarazione di elementi attivi inferiori a quelli reali.

Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 d.lgs. 74/2000) Commette il reato chi, al fine di consentire a terzi l'evasione delle imposte sui redditi o l'IVA, emette o rilascia fatture o altri documenti per operazioni inesistenti.

L'emittente delle fatture o dei documenti e chi partecipa alla commissione di tale reato non sono punibili anche a titolo di concorso nel reato di dichiarazione fraudolenta commesso dal terzo che si avvale di tali documenti, così pure tale terzo non è punibile anche a titolo di concorso nel reato di emissione in oggetto.

Occultamento o distruzione di documenti contabili (art. 10 d.lgs. 74/2000) Il reato è commesso da chi, al fine di evadere le imposte sui redditi o l'IVA o di consentirne l'evasione da parte di terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da impedire la ricostruzione dei redditi o del volume d'affari.

Sottrazione fraudolenta al pagamento di imposte (art. 11 d.lgs. 74/2000) La condotta punita consiste nel compimento, sui beni propri o di terzi, di atti dispositivi simulati o fraudolenti, idonei a rendere incapiente la procedura di riscossione coattiva delle imposte sui redditi dell'IVA, di interessi o sanzioni amministrative relativi a tali imposte, per un ammontare complessivo superiore a 50 mila euro. È altresì punita la condotta di chi nell'ambito di una procedura di transazione fiscale, al fine di ottenere per sé o per altri un minor pagamento di tributi e accessori, indica nella documentazione presentata elementi attivi inferiori a quelli reali o elementi passivi fittizi per un ammontare complessivo superiore a 50 mila euro.

Dichiarazione infedele (art. 4 D.lgs. 74/2000) Si configura quando, al fine di evadere le imposte sui redditi o sull'IVA, sono indicati nella dichiarazione annuale elementi attivi inferiori a quelli effettivi o elementi passivi fittizi, superando determinate soglie di rilevanza penale.

Omessa dichiarazione (art. 5, D.lgs. 74/2000) Integrata nel caso in cui, pur essendo obbligato, il contribuente non presenti la dichiarazione dei redditi o dell'IVA entro i termini previsti dalla legge, qualora l'imposta evasa superi determinati limiti.

Indebita Compensazione (art. 10-quater D.LGS. 74/2000) Il reato in oggetto è commesso da chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, ovvero addirittura fittizi, per un importo annuo superiore a cinquantamila euro. Tale reato assume rilevanza ai sensi del Decreto 231 se commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

6.2. Le Attività Aziendali sensibili

La Società ha individuato le seguenti attività come sensibili al rischio di commissione di reati tributari:
1) Gestione degli adempimenti fiscali
2) Gestione della Contabilità;
3) Gestione delle Operazioni societarie;
4) Selezione e gestione dei fornitori.

Per quanto riguarda i rapporti con i terzi, quali clienti, fornitori, partner e controparti in genere al fine di mitigare il rischio di essere coinvolta in illeciti fiscali dei medesimi, considerato anche che la legge, ai sensi dell'art. 13 bis del D. Lgs. n. 74/2000, punisce più severamente gli intermediari bancari e finanziari che concorrono nell'elaborazione o nella commercializzazione di modelli di evasione fiscale, la Società ha altresì predisposto i protocolli che disciplinano le seguenti attività, già descritti all'interno delle specifiche sezione del Modello:

- Gestione delle procedure acquisitive dei beni e dei servizi, in particolare la selezione e gestione dei fornitori;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni
- Acquisto, gestione e cessione di partecipazioni e di altri asset,
- compresa la strutturazione di operazioni straordinarie;
- Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose;

6.3. Predisposizione delle dichiarazioni fiscali e gestione degli adempimenti tributari

Tale attività è svolta centralmente dalla Casa Madre che gestisce la fiscalità consolidata. Tuttavia, la sede secondaria italiana fornisce supporto operativo, in particolare attraverso:

- la raccolta e verifica documentale delle informazioni fiscali relative alle operazioni locali;
- la trasmissione dei dati contabili e fiscali alla Casa Madre, garantendone correttezza, completezza e tempestività;
- il dialogo con i consulenti fiscali locali ove necessario.

6.4. Contabilità e fatturazione passiva

La sede secondaria italiana si occupa del primo livello di controllo del ciclo passivo, secondo il seguente processo:
- Le fatture elettroniche dei fornitori vengono ricevute tramite SDI nella casella PEC dell'Agenzia delle Entrate;
- Vengono scaricate e registrate in un apposito registro interno;
- Si effettua una verifica preliminare sulla coerenza tra il contratto sottoscritto e il regime fiscale applicato (es. imponibilità IVA, ritenute, ecc.);
- Viene consultato, ove necessario, il team Finance per chiarimenti o validazioni;
- Le fatture vengono trasmesse alla Casa Madre che le inserisce nella piattaforma gestionale esterna, dove sono sottoposte a ulteriori controlli

automatici e procedurali.

6.5. Operazioni societarie

La gestione delle operazioni straordinarie e societarie (fusioni, acquisizioni, cessioni, riorganizzazioni) è di competenza esclusiva della Casa Madre. La sede secondaria italiana ha esclusivamente una funzione di supporto operativo e di business, senza potere decisionale o esecutivo.

6.6. Selezione e gestione dei fornitori

La fase di selezione e onboarding dei fornitori è regolata da una specifica procedura aziendale di Know Your Counterparty (KYC**)**, che include anche controlli di tipo fiscale e reputazionale. L'applicazione della procedura è centralizzata, ma la sede italiana collabora al processo di verifica, segnalando eventuali anomalie o incoerenze riscontrate nella documentazione.

6.7. Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari

6.7.1 Premessa

Il presente protocollo si applica a tutte le strutture della Sede Secondaria coinvolte nella gestione dei rischi. e degli adempimenti ai fini della prevenzione dei reati tributari.
Ai sensi del D. Lgs. n. 231/2001, il processo potrebbe presentare occasioni per la commissione dei seguenti reati tributari: "*Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti*", "*Dichiarazione fraudolenta mediante altri artifici*", "*Emissione di fatture o altri documenti per operazioni inesistenti"*, "*Occultamento o distruzione di documenti contabili"* e di "*Sottrazione fraudolenta al pagamento di imposte*". Inoltre, le regole aziendali e i controlli di completezza e di veridicità previsti nel presente protocollo sono predisposti anche al fine di una più ampia azione preventiva dei reati che potrebbero conseguire a una scorretta gestione delle risorse finanziarie, quali i reati "*Riciclaggio*" e di "*Autoriciclaggio*".
Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.
Il presente protocollo a tutte le Strutture coinvolte nella gestione dei rischi in materia fiscale e alle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalle altre sedi del Gruppo e/o *outsourcer* esterni.

6.7.2 Descrizione del processo

Il processo di gestione dei rischi e degli adempimenti ai fini della prevenzione

dei reati tributari interessa, in modo diretto e/o indiretto, una serie eterogenea di processi aziendali che riguardano:

- le fasi di acquisto e di vendita di beni e servizi;
- la rappresentazione dei fatti di gestione nella contabilità e nei sistemi aziendali,
- la predisposizione delle dichiarazioni fiscali e la corretta liquidazione/riversamento delle relative imposte;

La rappresentazione dei fatti di gestione nella contabilità e nei sistemi aziendali, ivi compresa la valutazione delle singole poste, è regolata dal protocollo "*Gestione dell'informativa periodica*".

I rapporti con le Autorità di Supervisione in materia fiscale (Agenzia delle Entrate) sono regolati in base alle regole operative sancite dalla normativa interna per la gestione dei rapporti con le Autorità di Supervisione e dal protocollo "*Gestione dei rapporti con le Autorità di Vigilanza*".

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna, sviluppata e aggiornata a cura delle strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

6.7.3 Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito del processo:
  - tutti i soggetti che intervengono nella gestione delle attività inerenti alla predisposizione delle dichiarazioni fiscali, e nelle prodromiche attività di emissione / contabilizzazione delle fatture: sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
  - nel caso in cui intervengano consulenti esterni/fornitori, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali; operano esclusivamente nell'ambito del perimetro di attività loro assegnato dal Responsabile della struttura di riferimento; ogni accordo/convenzione con l'Agenzia delle Entrate è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
  - nei casi in cui l'orientamento fiscale che la Sede Secondaria intende adottare non dovesse essere condiviso dall'Agenzia delle Entrate, la sua definitiva adozione deve essere approvata dal Consiglio di Amministrazione, previa valutazione del Responsabile della Funzione fiscale in ordine ai rischi e ai costi/benefici derivanti dalla posizione che si intende assumere e acquisizione del parere di almeno un autorevole consulente fiscale esterno.

- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi di gestione dei rischi i e degli adempimenti ai fini della prevenzione dei reati tributari. In particolare:
  - le attività di cui alle diverse fasi del processo devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere

supportate da un meccanismo di *maker* e *checker*.

- Attività di controllo:
  - controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle autorità fiscali da parte della Struttura interessata per le attività di competenza che devono essere supportate da meccanismi di *maker* e *checker*;
  - controlli di carattere giuridico sulla conformità alla normativa di riferimento della dichiarazione fiscale;
  - controlli automatici di sistema, con riferimento alle dichiarazioni periodiche;
  - controlli sulla corretta emissione, applicazione delle aliquote IVA e contabilizzazione delle fatture del ciclo attivo e sulla loro corrispondenza con i contratti e impegni posti in essere con i terzi;
  - controlli sull'effettività, sia dal punto di vista soggettivo che oggettivo, del rapporto sottostante alle fatture passive ricevute e sulla corretta registrazione e contabilizzazione.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ciascuna fase rilevante del processo di gestione del rischio e degli adempimenti ai fini della prevenzione dei reati tributari deve risultare da apposita documentazione scritta;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.

- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

6.7.4 Principi di comportamento

Le strutture della Sede Secondaria, a qualsiasi titolo coinvolte nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari oggetto del protocollo come pure tutti i dipendenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna, nonché le eventuali le previsioni del Codice Etico.
Per prevenire il rischio di commissione di reati tributari, tutti i destinatari dovranno attenersi ai seguenti princìpi di condotta:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle regole aziendali interne, in tutte le Attività Sensibili individuate nella presente Parte Speciale;
2. agevolare il monitoraggio del rispetto dei princìpi che regolano la compilazione, tenuta e conservazione delle dichiarazioni di natura contabile rilevanti ai fini fiscali;
3. conservare in modo adeguato delle scritture contabili e degli altri documenti

di cui sia obbligatoria la conservazione ai fini fiscali;
4. attuare la cosiddetta "segregazione dei ruoli" nella gestione delle contabilità aziendale e nel processo di predisposizione delle dichiarazioni fiscali;
5. garantire la massima correttezza nell'ambito dei rapporti con l'amministrazione fiscale e la massima trasparenza nella comunicazione di dati e informazioni alla stessa.

In particolare, tutti le Strutture sono tenute - nei rispettivi ambiti - a:
- garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari della Società nelle dichiarazioni fiscali;
- rispettare i principi di condotta in materia fiscale al fine di (i) garantire nel tempo la conformità alle regole fiscali e tributarie dei Paesi dove la Sede Secondaria opera e, (ii) l'integrità patrimoniale e la reputazione del Gruppo;
- agire secondo i valori dell'onestà e dell'integrità nella gestione della variabile fiscale, nella consapevolezza che il gettito derivante dai tributi costituisce una delle principali fonti di contribuzione allo sviluppo economico e sociale dei Paesi in cui opera;
- garantire la diffusione di una cultura aziendale improntata ai valori di onestà e integrità e al principio di legalità;
- mantenere un rapporto collaborativo e trasparente con l'Autorità Fiscale garantendo a quest'ultima, tra l'altro, la piena comprensione dei fatti sottesi all'applicazione delle norme fiscali;
- eseguire gli adempimenti fiscali nei tempi e nei modi definiti dalla normativa o dall'autorità fiscale;
- evitare forme di pianificazione fiscale che possano essere giudicate aggressive da parte delle autorità fiscali;
- interpretare le norme in modo conforme al loro spirito e al loro scopo rifuggendo da strumentalizzazioni della loro formulazione letterale;
- rappresentare gli atti, i fatti e i negozi intrapresi in modo da rendere applicabili forme di imposizione fiscale conformi alla reale sostanza economica delle operazioni;
- garantire trasparenza alla propria operatività e alla determinazione dei propri redditi e patrimoni evitando l'utilizzo di strutture, anche di natura societaria, che possano occultare l'effettivo beneficiario dei flussi reddituali o il detentore finale dei beni;
- rispettare le diposizioni atte a garantire idonei prezzi di trasferimento per le operazioni infragruppo con la finalità di allocare, in modo conforme alla legge, i redditi generati;
- collaborare con le autorità competenti per fornire in modo veritiero e completo le informazioni necessarie per l'adempimento e il controllo degli obblighi fiscali;
- stabilire rapporti di cooperazione con le amministrazioni fiscali, ispirati alla trasparenza e fiducia reciproca e volti a prevenire i conflitti, riducendo quindi la possibilità di controversie;
- proporre alla clientela prodotti e servizi che non consentano di conseguire indebiti vantaggi fiscali non altrimenti ottenibili, prevedendo inoltre idonee forme di presidio per evitare il coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato

considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità Fiscali in errore;
- procedere con il pagamento di una fattura senza verificare preventivamente l'effettività, la qualità, la congruità e tempestività della prestazione ricevuta e l'adempimento di tutte le obbligazioni assunte dalla controparte;
- utilizzare strutture o società artificiose, non correlate all'attività imprenditoriale, al solo fine di eludere la normativa fiscale;
- emettere fatture o rilasciare altri documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- indicare nelle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto: i) elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti; ii) elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi (ad esempio costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento; iii) una base imponibile in misura inferiore a quella effettiva attraverso l'esposizione di elementi attivi per un ammontare inferiore a quello reale o di elementi passivi fittizi; iv) fare decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle medesime così come per il successivo versamento delle imposte da esse risultanti.

I Responsabili delle Strutture interessate della Sede Secondaria sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

6.7.5 Controlli Dell'organismo Di Vigilanza

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei Destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e princìpi contenuti nella presente Parte Speciale.
In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei princìpi contenuti nelle policy aziendali adottate ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

L'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai princìpi procedurali specifici contenuti nella presente Parte Speciale ovvero alle procedure, *policy* e normative aziendali attinenti alle Attività Sensibili sopra individuate.
È, altresì, attribuito all'OdV il potere di accedere o di richiedere ai propri delegati

di accedere a tutta la documentazione e a tutti i siti aziendali rilevanti per lo svolgimento dei propri compiti.

6.8. Flussi informativi nei confronti dell'organismo di vigilanza

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.
- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua verifiche semestrali, ad evento e annuali.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	**Descrizione del flusso informativo**	**Periodicità**
Finance	Comunicazione di rilievi fiscali ricevuti, utilizzo di crediti d'imposta, compensazioni effettuate	Ad evento
Finance	Comunicazione su fornitori a rischio, anomalie nella documentazione fiscale ricevuta, operazioni sospette	Ad evento
Compliance	Informative su ispezioni tributarie, verbali di constatazione, avvisi bonari o accertamenti	Ad evento
Corporate Affairs	Invio verbali e documentazione su operazioni straordinarie societarie con impatto fiscale	Ad evento

7. REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI ED UTILITÀ DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO - REATI CON FINALITA' DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO – DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

7.1. Premessa

La presente Parte Speciale ha l'obiettivo di illustrare i criteri, i ruoli e le responsabilità, i principi di controllo e le regole di comportamento cui tutti i Destinatari, ivi compresi i consulenti, i dipendenti, i fornitori e i partner, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dagli articoli 25-*octies* e 25-*quater* del Decreto, nel rispetto dei principi di legalità, correttezza, oggettività, trasparenza,
tracciabilità e riservatezza nell'esecuzione delle proprie attività, della normativa emanata dagli organismi di vigilanza e di tutte le leggi e le norme nazionali ed internazionali vigenti.
Tale Parte Speciale compendia, altresì, i principi volti a prevenire la commissione dei delitti previsti dall'art. *25-octies.1* del Decreto introdotti dal D. Lgs. n. 8.11.2021, n. 184 in recepimento alla Direttiva (UE) 2019/713 *"relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti*").

7.2. Le fattispecie di reato di cui agli artt. 25-octies, 25-octies.1. e 25-quater del Decreto

Il D. Lgs. 21.11.2007, n. 231 (di seguito Decreto antiriciclaggio) e il D. Lgs. 22.6.2007 n. 109, in attuazione di disposizioni comunitarie hanno rafforzato la normativa in tema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di contrasto al finanziamento del terrorismo.
L'art. 25-octies del D. Lgs. 231/2001, introdotto dal Decreto antiriciclaggio ha esteso la responsabilità dell'Ente ai reati di ricettazione, riciclaggio anche per le ipotesi in cui non siano commessi con finalità di terrorismo o di eversione dell'ordine democratico - trattate al paragrafo 7 - o non presentino le caratteristiche di transnazionalità in precedenza previste. Da ultimo, l'art. 25-octies è stato modificato aggiungendovi il nuovo reato di autoriciclaggio.

Il rafforzamento della disciplina della responsabilità amministrativa degli Enti intende prevenire e reprimere più efficacemente il fenomeno dell'immissione nel circuito economico lecito di denaro, beni od utilità provenienti dalla commissione di delitti, in quanto di ostacolo all'amministrazione della giustizia nelle attività di accertamento dei reati e di persecuzione dei colpevoli, oltre che, più in generale, lesiva dell'ordine economico, dell'integrità dei mercati e della libera concorrenza,

in ragione degli indebiti vantaggi competitivi di cui godono gli operatori che dispongono di capitali di origine illecita.
Su un piano diverso, ma pur sempre finalizzate al contrasto del riciclaggio e del finanziamento del terrorismo, si collocano le previsioni contenute nel Decreto antiriciclaggio di specifici adempimenti posti a carico delle banche, degli intermediari finanziari e di altri determinati soggetti obbligati (adeguata verifica della clientela; registrazione e conservazione della documentazione delle operazioni; segnalazione di operazioni sospette; comunicazioni delle violazioni dei divieti in tema di denaro contante e dei titoli al portatore; comunicazione da parte degli Organi di controllo dell'Ente delle infrazioni riscontrate). La violazione di detti obblighi di per sé non comporta la responsabilità amministrativa dell'Ente ai sensi del D. Lgs. 231/2001, non essendo detti illeciti ricompresi nell'elencazione dei cosiddetti reati presupposto ma è sanzionata ai sensi del Decreto antiriciclaggio secondo una politica di tutela preventiva che prescinde dal ricorrere nelle concrete fattispecie di ipotesi di riciclaggio, ma che mira comunque ad assicurare il rispetto dei fondamentali principi della approfondita conoscenza della clientela e della tracciabilità delle transazioni, al fine di scongiurare anche il mero pericolo di inconsapevole coinvolgimento in attività illecite.
È importante sottolineare che qualora l'operatore della Sede Secondaria contravvenisse a detti adempimenti nella consapevolezza della provenienza illecita dei beni oggetto delle operazioni, potrebbe essere chiamato a rispondere per i predetti reati, e potrebbe quindi conseguirne anche la responsabilità amministrativa della Sede Secondaria ai sensi del D. Lgs. 231/2001.
Il D. Lgs. 08.11.2021, n. 195 in attuazione della Direttiva (UE) 2018/1673 "*relativa alla lotta al riciclaggio mediante il diritto penale*" ha modificato il tessuto di tipicità dei reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648- *bis* c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.) nonché di autoriciclaggio (art. 648-*ter*.1. c.p.), ampliando il novero dei reati presupposto anche alle contravvenzioni (laddove punite con la pena dell'arresto superiore nel massimo a un anno ovvero nel minimo a 6 mesi) e includendo i delitti colposi come presupposto delle fattispecie di riciclaggio e autoriciclaggio.
L'ampliamento del perimetro di rilevanza di tale fattispecie determina una dilatazione dell'area di rilevanza anche dei rispettivi illeciti amministrativi dipendenti da reato richiamati dall'art. 25-*octies* del D. Lgs. 231/2001.
Sul punto è doveroso, inoltre, segnalare un contrasto giurisprudenziale, ed infatti, il principio di tassatività dei reati che possono comportare la responsabilità dell'ente è stato messo in discussione da un recente orientamento interpretativo dottrinale emerso in relazione al reato- presupposto di autoriciclaggio. Da un lato, un primo orientamento statuisce che la responsabilità ai sensi del D. Lgs. n. 231/2001 sarebbe limitata ai casi in cui il reato-base dell'autoriciclaggio sia anche un reato presupposto enucleato nel Decreto; dall'altro lato, un secondo orientamento postula la configurabilità di tale responsabilità anche in presenza di ulteriori fattispecie di reato-base, con la conseguenza che l'ente potrebbe incorrere in tale responsabilità anche in relazione a reati estranei al catalogo previsto dal Legislatore. In questa ultima ipotesi, come evidenziato anche nelle Linee Guida di Confindustria – pubblicate nel mese di giugno 2021 – "*tale catalogo perderebbe la natura tassativa e risulterebbe integrato attraverso il rinvio indeterminato a ulteriori fattispecie di reato, con la conseguente difficoltà di predisporre adeguate misure di prevenzione e il rischio di allargare l'ambito di*

applicazione dei Modelli 231 a ulteriori aree di compliance non ricomprese nell'ambito del Decreto 231". Tale orientamento viene ulteriormente ribadito posto che l'esigenza di garantire il rispetto di principi fondamentali quali quello di legalità e tassatività dell'elenco dei reati-presupposto della responsabilità degli enti nascente da reato, determina la necessità di circoscrivere in via interpretativa l'elenco dei possibili delitti – ora anche di natura colposa – che possono determinare tale responsabilità a quelli già previsti dal
D. Lgs. n. 231/2001.

Inoltre. Il D. Lgs. 8.11. 2021, n. 184 (in recepimento alla Direttiva (UE) 2019/713 "*relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti*") ha introdotto il nuovo articolo 25-*octies.*1, rubricato "*Delitti in materia di strumenti di pagamento diversi dai contanti*" introducendo nel catalogo dei reati presupposto le seguenti fattispecie:

i. indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti, ai sensi del novellato art. 493-*ter* c.p.
ii. detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti, ai sensi del neo-introdotto art. 493- *quarter* c.p.;
iii. frode informatica (art. 640-*ter* c.p.) non solo se commessa ai danni dello Stato o di altro ente pubblico o dell'Unione Europea, come già previsto dall'art. 24 del Decreto ma, altresì, "*nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale*";
iv. qualsivoglia delitto contro la fede pubblica o contro il patrimonio posto in essere attraverso l'impiego di strumenti di pagamento diversi dal contante.

È opportuno precisare che per "*strumenti di pagamento diversi dai contanti*" si intende "*un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali*".

Si fornisce qui di seguito una sintetica descrizione degli elementi costitutivi dei reati in oggetto.

Ricettazione (art. 648 c.p.) Commette il reato di ricettazione chiunque, fuori dai casi di concorso nel reato, allo scopo di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, alla cui commissione non ha partecipato, o comunque si intromette nel farli acquistare, ricevere od occultare. Per tale reato è richiesta la presenza di dolo specifico da parte di chi agisce, e cioè la coscienza e la volontà di trarre profitto, per sé stessi o per altri, dall'acquisto, ricezione od occultamento di beni di provenienza delittuosa.
E' inoltre richiesta la conoscenza della provenienza delittuosa del denaro o del bene; la sussistenza di tale elemento psicologico potrebbe essere riconosciuta in presenza di circostanze gravi ed univoche - quali ad esempio la qualità e le caratteristiche del bene, le condizioni economiche e contrattuali inusuali dell'operazione, la condizione o la professione del possessore dei beni - da cui possa desumersi che nel soggetto che ha agito poteva formarsi la certezza della

provenienza illecita del denaro o del bene. Il D. Lgs 8.11.2021 n. 195 ha configurato quale reato presupposto anche le contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

Riciclaggio (art. 648-bis c.p.) Tale ipotesi di reato si configura nel caso in cui il soggetto agente, che non abbia concorso alla commissione del delitto sottostante, sostituisca o trasferisca denaro, beni od altre utilità provenienti da un delitto non colposo, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.
La norma va interpretata come volta a punire coloro che - consapevoli della provenienza delittuosa di denaro, beni o altre utilità - compiano le operazioni descritte, in maniera tale da creare in concreto difficoltà alla scoperta dell'origine illecita dei beni considerati.
Non è richiesto, ai fini del perfezionamento del reato, l'aver agito per conseguire un profitto o con lo scopo di favorire gli autori del reato sottostante ad assicurarsene il provento. Costituiscono riciclaggio le condotte dinamiche, atte a mettere in circolazione il bene, mentre la mera ricezione od occultamento potrebbero integrare il reato di ricettazione. Con riferimento ai rapporti bancari, ad esempio, la semplice accettazione di un deposito potrebbe integrare la condotta di sostituzione tipica del riciclaggio (sostituzione del denaro contante con moneta scritturale, quale è il saldo di un rapporto di deposito).
Come per il reato di ricettazione, la consapevolezza dell'agente in ordine alla provenienza illecita può essere desunta da qualsiasi circostanza oggettiva grave ed univoca.
Il sopracitato D. Lgs. 8.11.2021, n. 195, prevede la configurabilità della fattispecie – seppur con un regime sanzionatorio meno afflittivo – nelle ipotesi in cui la condotta delittuosa riguardi denaro ovvero beni provenienti da fattispecie contravvenzionali punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) La condotta criminosa si realizza attraverso l'impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto, fuori dei casi di concorso nel reato d'origine e dei casi previsti dagli articoli 648 (ricettazione) e 648-bis (riciclaggio) c.p.
A seguito delle modifiche introdotte dal D. Lgs. 8.11.2021, n. 195, sono state inoltre ricomprese nel novero delle fattispecie presupposto anche le contravvenzioni punite con l'arresto superiore nel massimo ad un anno o nel minimo a sei mesi.
Rispetto al reato di riciclaggio, pur essendo richiesto il medesimo elemento soggettivo della conoscenza della provenienza illecita dei beni, l'art. 648 ter circoscrive la condotta all'impiego di tali risorse in attività economiche o finanziarie. Peraltro, in considerazione dell'ampiezza della formulazione della fattispecie del reato di riciclaggio, risulta difficile immaginare condotte di impiego di proventi illeciti che già non integrino di per sé il reato di cui all'art. 648 bis c.p.

Autoriciclaggio (art. 648-ter.1 c.p.) Risponde del reato di autoriciclaggio chi, avendo commesso o concorso a commettere un qualsiasi delitto non colposo dal quale provengono denaro, beni, o altre utilità, su tali proventi compie operazioni di impiego, sostituzione o trasferimento in attività economiche,

finanziarie, imprenditoriali o speculative, con modalità tali da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
È esclusa la punibilità delle condotte consistenti nella destinazione dei proventi illeciti alla mera utilizzazione o godimento personale. È prevista un'aggravante di pena se il fatto è commesso nell'esercizio di attività professionale, bancaria o finanziaria e un'attenuante per il caso di ravvedimento operoso del reo.
Il D.lgs. 8.11.2021, n. 195 ha ampliato il catalogo dei reati base, prevedendo la configurabilità degli stessi anche a titolo colposo, nonché anche nelle ipotesi in cui la fattispecie base sia una contravvenzione punita con l'arresto superiore nel massimo a un anno ovvero nel minimo a sei mesi, seppur configurando un regime sanzionatorio meno afflittivo.

Considerazioni comuni ai reati.
Oggetto materiale.
L'oggetto materiale dei reati può essere costituito da qualsiasi entità economicamente apprezzabile e possibile oggetto di scambio, quale il denaro, i titoli di credito, i mezzi di pagamento, i diritti di credito, i preziosi, i beni materiali ed immateriali in genere. Deve però trattarsi di bene o utilità proveniente da delitto, vale a dire esso ne deve costituire il prodotto (risultato, frutto ottenuto dal colpevole con la commissione del reato), il profitto (lucro o vantaggio economico ricavato dal reato) o il prezzo (compenso dato per indurre, istigare, determinare taluno alla commissione del reato). Oltre che i delitti tipicamente orientati alla creazione di capitali illeciti (ad es.: concussione, corruzione, appropriazione indebita, truffa, reati fallimentari, traffico di armi o di stupefacenti, usura, frodi comunitarie, ecc.), anche i reati in materia fiscale potrebbero generare proventi oggetto di riciclaggio o di autoriciclaggio, non solo nel caso di frodi (ad es. utilizzo di fatture per operazioni inesistenti che determinino un fittizio credito Iva da detrarre), ma anche nel caso in cui l'utilità economica conseguente al reato consista in un mero risparmio di imposta per mancato esborso di denaro proveniente da attività lecite (ad es., omessa o infedele dichiarazione di redditi, per importi oltre le soglie di rilevanza penale).
Sul punto si precisa come il D.Lgs. 8.11.2022, n. 195 abbia ampliato il catalogo dei reati base, prevedendo in taluni casi la configurabilità degli stessi anche a titolo colposo nonché, in talaltri, anche nelle ipotesi in cui la fattispecie base sia una contravvenzione punita con l'arresto superiore nel massimo a un anno ovvero nel minimo a sei mesi, seppur configurando un regime sanzionatorio meno afflittivo.
Condotta ed elemento soggettivo.
Risponde dei reati di ricettazione, riciclaggio o reimpiego illecito, a seconda dei casi, il terzo estraneo al delitto che genera i proventi illeciti e che li riceva dal reo (o da altri, comunque conoscendone la provenienza illecita), per compiere su di essi le condotte previste dai reati medesimi.
Potrebbe invece rispondere a titolo di concorso nel delitto d'origine dei proventi illeciti e, di conseguenza, anche nel successivo reato di autoriciclaggio, qualora ne realizzi la condotta, il soggetto che avesse fornito un contributo causale di qualsiasi tipo, morale o materiale, alla commissione del reato d'origine, ad es. determinando o rafforzando il proposito criminoso del reo con la promessa, ancor prima della commissione del reato, del suo aiuto nel riciclare/impiegare i proventi.
Il reato di autoriciclaggio, diversamente da quanto previsto per i reati di

riciclaggio e di impiego illecito, richiede che la condotta sia caratterizzata da modalità idonee a concretamente mascherare la vera provenienza delittuosa dei beni; l'interpretazione degli aspetti più innovativi della norma
- vale a dire il requisito del concreto ostacolo e la condizione di non punibilità dell'auto riciclatore ad uso personale (che sembrerebbe sempre da escludersi allorché il reato d'origine e il reimpiego avvengano nell'esercizio di un'attività d'impresa) - sarà necessariamente demandata alle applicazioni giurisprudenziali del nuovo reato.

Circa l'elemento soggettivo, come già accennato, i reati in esame devono essere caratterizzati dalla consapevolezza della provenienza delittuosa del bene. Secondo una interpretazione particolarmente rigorosa, sarebbe sufficiente anche l'aver agito nel dubbio della provenienza illecita, accettandone il rischio (cosiddetto dolo indiretto od eventuale). Con riferimento all'operatività della Sede Secondaria va osservato che la presenza in determinate situazioni concrete di indici di anomalia o di comportamenti anomali descritti nei provvedimenti e negli schemi emanati dalle competenti Autorità (per quanto concerne gli intermediari finanziari, dalla Banca d'Italia e dall'UIF) potrebbe essere ritenuta, accedendo alla particolarmente rigorosa interpretazione di cui sopra, come una circostanza oggettiva grave ed univoca atta far sorgere il dubbio dell'illecita provenienza del bene.

Correlazioni col reato d'origine dei proventi illeciti.

I reati della presente Area sensibile sussistono nelle ipotesi in cui le relative condotte siano successive al perfezionamento del reato che ha dato origine ai proventi illeciti, anche se compiute dopo la sua estinzione (ad es. per prescrizione o morte del reo), o anche se l'autore del medesimo non sia imputabile o punibile, oppure manchi una condizione di procedibilità (ad es., per difetto di querela, oppure di richiesta del Ministro della Giustizia, necessaria per perseguire i reati comuni commessi all'estero, ai sensi degli artt. 9 e 10 c.p.).

Di seguito si illustrano, altresì, i reati presupposto elencati dall'art. 25-*octies*.1 del D. Lgs. n. 231/2001.

Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-*ter* c.p.) Tale fattispecie sanziona l'indebita utilizzazione, da parte di chi non ne è titolare, di carte di credito o pagamento o di qualsiasi altro documento analogo che abiliti al prelievo di contante, all'acquisto di beni o alla prestazione di servizi, o comunque di ogni altro strumento di pagamento diverso dai contanti; la falsificazione o l'alterazione dei medesimi documenti o strumenti; il possesso, la cessione ovvero l'acquisizione degli strumenti e dei documenti descritti, ove di provenienza illecita, o di ordini di pagamento prodotti con essi.

Il reato potrebbe essere astrattamente integrato qualora un esponente della Società (apicale ovvero subordinato), nell'interesse o a vantaggio della stessa, falsifichi o utilizzi illecitamente uno strumento di pagamento diverso dai contanti (es. carte di credito/debito aziendali) che consenta al titolare o all'utilizzatore di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali).

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-*quater* c.p.) Si tratta di una fattispecie sussidiaria e la condotta consiste nel produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo

procurare a sé o ad altri l'oggetto materiale del reato. Quest'ultimo può essere costituito da apparecchiature, dispositivi informatici (hardware, chiavi USB, CD-ROM, dvd, hard disk esterni, ecc.) nonché programmi informatici (cosiddetti *software)* la cui finalità è quella di commettere reati riguardanti strumenti di pagamento alternativi ai contanti. La condotta si caratterizza per essere finalizzata a consentire l'uso ovvero a permettere l'utilizzo da parte di altri delle apparecchiature, dispositivi o programmi informatici predisposti o adattati proprio per commettere reati riguardanti i già menzionati strumenti alternativi di pagamento.

Frode informatica aggravata (art. 640-ter c.p.) Il reato di frode informatica è già previsto nel catalogo dei reati presupposto ai sensi dell'art. 24 del Decreto, qualora sia commesso in danno dello Stato o di altro ente pubblico o dell'Unione europea (art. 640 *ter,* comma 2, c.p.). Il D. Lgs. 8.11.2021, n. 184 è stata introdotta una circostanza aggravante qualora la condotta produca un trasferimento di denaro, di valore monetario o di valuta virtuale.

Trasferimento fraudolento di valori (art. 512-bis c.p. articolo introdotto dalla L. n. 137/2023 e modificato dal D.L. 19/2024) La fattispecie punisce chiunque, attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648 648-bis e 648-ter

Altri reati aventi ad oggetto strumenti di pagamento diversi dai contanti
Per la prima volta nella costruzione di una norma concernente i reati presupposto, non vengono specificatamente identificate le fattispecie di reato rilevanti posto che il Legislatore si è limitato ad un richiamo generico
a categorie di reati individuate in ragione del bene giuridico tutelato dalla norma incriminatrice, sanzionando la commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale a condizione, che l'azione ovvero l'omissione illecita si ponga in relazione a "*strumenti di pagamento diversi dai contanti"*.

Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater del D.Lgs. 231/2001) Sono considerati reati rilevanti ai sensi dell'art. 25-quater del D.Lgs. 231/2001 i delitti commessi con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali.

Tra questi rientrano:

Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-bis c.p.) Il reato punisce chi promuove, costituisce, organizza, dirige o partecipa ad associazioni che si propongono il compimento di atti di violenza con finalità terroristiche o eversive dell'ordine democratico.

Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinquies c.p.) Il Reato punisce chiunque, al di fuori dei casi di cui all´articolo 270-bis, addestra o comunque fornisce istruzioni sulla preparazione o sull´uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un´istituzione o un organismo internazionale

Detenzione di materiale con finalità di terrorismo (art. 270-quinquies.3 c.p., introdotto dal D.L. n.48/2025 convertito dalla L.n.80/ 2025) Il Reato punisce chiunque, al di fuori dei casi previsti dall'art. 270-quinquies, detiene, fabbrica, importa, esporta o comunque mette a disposizione materiale, sostanze o apparati idonei per il compimento di atti con finalità terroristiche.

Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.) Tale reato punisce chiunque raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo

Fabbricazione o detenzione di materie esplodenti (art. 435 c.p., introdotto dal D.L. n.48/2025 convertito dalla L.n. 80/ 2025) Tale reato punisce chiunque, al fine di attentare alla pubblica incolumità, fabbrica, acquista o detiene dinamite o altre materie esplodenti, asfissianti, accecanti, tossiche o infiammabili, ovvero sostanze che servano alla composizione o alla fabbricazione di esse.

7.3. Attività Aziendali sensibili

Il rischio che si verifichino nel contesto della Sede Secondaria i reati di riciclaggio, intesi in senso lato (ivi compreso, quindi, l'autoriciclaggio), appare invero, più marcato, quale rischio tipico del circuito bancario e finanziario, essenzialmente con riferimento ai rapporti con la clientela, e ad ipotesi di coinvolgimento/concorso in attività criminose della stessa in particolare concerne:

- l'instaurazione e la gestione dei rapporti continuativi con la clientela;
- il trasferimento di fondi.

L'attività di prevenzione si basa sulla approfondita conoscenza della clientela e delle controparti e sulla osservanza degli adempimenti previsti dalla normativa in tema di contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo.
La centralità del rispetto rigoroso delle disposizioni dettate dal Decreto antiriciclaggio ai fini della prevenzione dei reati presupposto in questione discende anche dalle considerazioni che seguono. Va innanzitutto ricordato che il Decreto - ai fini dell'individuazione della tipologia delle condotte con le quali può concretarsi il riciclaggio, sottoposte all'obbligo di segnalazione delle operazioni sospette - all'art. 1 definisce "operazione" la trasmissione o la movimentazione

di mezzi di pagamento" e all'art. 2 contiene un'elencazione di condotte, qualificate come di riciclaggio, di amplissima estensione, tale da comprendere comportamenti che, ai fini penali, potrebbero integrare la commissione del reato di autoriciclaggio, oppure la commissione degli altri reati presupposto in esame e che, se posti in essere da dipendenti o da soggetti apicali, potrebbero far sorgere la responsabilità amministrativa dell'ente stesso. Infine, l'elencazione in discorso è atta a ricomprendere anche condotte tipiche di altri reati, quali il favoreggiamento personale (art. 378 c.p.) che, se connotato dai requisiti della transnazionalità, può costituire anch'esso reato presupposto della responsabilità amministrativa degli Enti.
Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose. Si evidenzia altresì che nell'ambito di protocolli che regolano altre attività sensibili - quali la Gestione dei contenziosi e degli accordi transattivi (paragrafo 4.8), la Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali (paragrafo 4.9) e la Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni (paragrafo 4.10 - sono previsti alcuni principi di controllo e di comportamento ispirati al medesimo criterio dell'attenta valutazione di fornitori, consulenti e controparti contrattuali in genere, principi che esplicano la loro efficacia preventiva anche in relazione ai reati sopra illustrati.
Più in generale, tutti i protocolli del presente Modello, laddove tesi a prevenire la commissione di reati che possono generare proventi illeciti, si devono intendere predisposti anche al fine della prevenzione dei reati di riciclaggio in senso lato. Si richiamano soprattutto i protocolli relativi alle Aree sensibili concernenti i reati societari - in particolare il protocollo sulla Gestione dell'informativa periodica (paragrafo 3.4) - i reati informatici.
Inoltre, in ragione dell'avvenuta estensione della platea dei reati presupposto delle fattispecie di riciclaggio e di autoriciclaggio, particolare attenzione deve essere riservata alla gestione delle tematiche rilevanti in materia di salute e sicurezza sul lavoro.
Tutti i sopra menzionati protocolli si completano con la normativa aziendale di dettaglio che regolamenta le attività medesime e si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalle altre società del Gruppo, e/o da *outsourcer* esterni.

Il Modello individua due aree sensibili:

1. Il contrasto finanziario al terrorismo e al riciclaggio dei proventi da attività criminosa.

2. La gestione dei conti correnti e delle carte di pagamento.

7.4. Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose

7.4.1 Premessa

Il presente protocollo ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi di controllo e di comportamento per il contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose. Si intendono qui richiamate le vigenti disposizioni aziendali, ed in particolare le Linee guida della Casa Madre per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo e per la gestione degli embarghi, le Linee Guida per il contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo e per la gestione degli embarghi della Sede Secondaria e la normativa interna in materia tempo per tempo vigente.
Il presente protocollo si applica a tutte le strutture della Sede Secondaria coinvolte nelle attività sensibili sopra individuate nonché nelle attività di presidio dei rischi connessi alla normativa antiriciclaggio.
Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria della normativa vigente e dei principi di trasparenza, correttezza, oggettività, tracciabilità e riservatezza nell'esecuzione delle attività in oggetto.

7.4.2 Descrizione del Processo

Il processo di prevenzione del riciclaggio e del finanziamento del terrorismo in Younited è disciplinato da un sistema articolato di policy e procedure, sia a livello di Gruppo che a livello locale, al fine di recepire le normative specifiche di ciascun Paese in cui il gruppo opera.

Tra i presidi adottati vi sono:
- Policy di Gruppo Antiriciclaggio e Lotta al Finanziamento del Terrorismo ("AML-CFT") Procedura di onboarding che consente la selezione delle controparti mediante un approccio basato sul rischio
- Procedura per l'individuazione e gestione delle operazioni sospette (atipiche)
- Procedura sul congelamento dei beni.

Durante la fase di onboarding il cliente viene sottoposto a un processo di valutazione del rischio, che prevede l'utilizzo di un sistema di screening e monitoraggio (DowJones), finalizzato all'individuazione di PEP (Persone Politicamente Esposte) e altri soggetti ad alto rischio.

Gli alert generati dal sistema Dow Jones vengono analizzati dal dipartimento Antifrode AML, struttura di prima linea all'interno della funzione Operations, che effettua un primo livello di controllo.

In caso di operazioni sospette o comportamenti anomali, si attiva un processo di escalation che coinvolge il responsabile SOS della succursale, che effettua la valutazione finale e decide se procedere all'invio di una segnalazione di operazione sospetta (SOS) tramite il portale InfoStat-UIF o se archiviare la pratica, motivando la decisione.

È attualmente in fase di implementazione il progetto di gruppo AML Score, che attribuisce un punteggio di rischio ai clienti specificamente per i profili AML, in aggiunta al credit score, che è una procedura che verifica il merito creditizio. Questo sistema è operativo anche nella fase di monitoraggio continuo e viene aggiornato nel tempo.

Particolare attenzione è dedicata al monitoraggio di operazioni anomale come le estinzioni anticipate e i cambi di coordinate bancarie, considerati eventi a rischio sotto il profilo antiriciclaggio.

La funzione antiriciclaggio predispone annualmente una relazione sull'attività svolta, condivisa con la capogruppo e il country manager, e trasmessa alla Banca d'Italia.

Ai fini del contrasto al finanziamento del terrorismo e al riciclaggio dei proventi di attività criminose, si rimanda ai seguenti ambiti di operatività:

- identificazione e conoscenza della clientela e dei soggetti per conto dei quali i clienti operano, valutandone il profilo di rischio e cioè la probabilità di esposizione a fenomeni di riciclaggio o di finanziamento del terrorismo tramite una apposita procedura di profilatura. La valutazione della sussistenza di tale rischio si basa sulla stessa conoscenza dei clienti e tiene conto, in particolare, di aspetti oggettivi (attività svolte dai clienti, le operazioni da essi compiute e degli strumenti utilizzati) e di aspetti soggettivi (soggetti sottoposti ad obblighi rafforzati di adeguata verifica; soggetti insediati in Paesi/centri caratterizzati da regimi fiscali o antiriciclaggio privilegiati quali quelli individuati dal GAFI come "non cooperativi", etc.).Particolare attenzione deve essere posta nel rilevare il possibile coinvolgimento in operazioni o rapporti con soggetti (persone fisiche e giuridiche) censiti in liste pubbliche emanate in ambito nazionale e internazionale (liste ONU, UE, OFAC e liste MEF, ABI-UIF, di seguito tutte denominate per brevità "Black List");
- apertura di nuovi rapporti continuativi e aggiornamento/revisione delle informazioni sui clienti esistenti, finalizzati al rispetto del principio della "know your customer rule";
- monitoraggio dell'operatività e costante valutazione dei rischi di riciclaggio di denaro proveniente da attività illecite o di finanziamento del terrorismo, secondo tempistiche e modalità stabilite con riferimento al profilo di rischio assegnato;
- valutazione dell'operatività disposta dalla clientela riguardante soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi);
- assolvimento degli obblighi normativi in materia di registrazione dei rapporti continuativi e delle operazioni disposte dalla clientela e conservazione delle relative informazioni;
- reporting esterno indirizzato alle Autorità di Vigilanza e reporting interno ad esso finalizzate.

Le modalità operative per la gestione dei suddetti processi sono disciplinate

nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti. Tale normativa costituisce parte integrante e sostanziale del presente protocollo.

7.4.3 Principi di controllo

Il sistema di controllo a presidio dei processi sopra descritti si basa sui seguenti fattori:

- Responsabilità definite:
  - la normativa interna individua i soggetti e le Strutture responsabili dell'attivazione/gestione/ controllo dei processi sopra descritti;
  - È previsto un sistema di procedure antiriciclaggio e di contrasto al finanziamento del terrorismo adottato sia a livello di Gruppo che a livello locale, per assicurare coerenza e uniformità di applicazione delle misure di prevenzione.

- Segregazione dei compiti:

Il principio di segregazione prevede che il processo di gestione delle operazioni sospette segua un flusso di escalation interno, con la decisione finale affidata alla Responsabile della Succursale. Tutte le decisioni adottate, sono documentate e tracciate.

  - nelle situazioni individuate dalle disposizioni di legge e dalla normativa interna che impongono obblighi rafforzati di adeguata verifica della clientela, subordinazione dell'apertura di nuovi rapporti, del mantenimento di rapporti preesistenti e dell'esecuzione delle operazioni al rilascio di una autorizzazione da parte di una Struttura diversa da quella operativa;
  - in relazione alle attività di monitoraggio dell'operatività volte ad individuare operazioni potenzialmente sospette, esistenza di una segregazione in base alla quale:
    - le funzioni aziendali competenti monitorano le operazioni relative alla loro area di competenza, segnalando i movimenti anomali al responsabile della struttura per gli opportuni approfondimenti e/o segnalazioni;
    - l'ufficio competente, sulla scorta delle informazioni in proprio possesso, ovvero di segnalazioni pervenute dagli operatori provvede, se l'operazione risulta sospetta, alla segnalazione della stessa al Responsabile Delegato per la segnalazione delle operazioni sospette (Responsabile Aziendale Antiriciclaggio);
    - il Responsabile per la segnalazione delle operazioni sospette effettua l'analisi della segnalazione e svolge autonomamente le necessarie indagini sull'operazione sospetta, disponendo l'inoltro o meno delle segnalazioni alla competente Autorità.

- Attività di controllo: il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:
  - nell'ambito di una puntuale profilatura della clientela, verifica secondo un approccio risk based, all'atto dell'accensione del rapporto, da parte del Responsabile della Struttura competente, della correttezza e completezza dei dati censiti in anagrafe, nonché in merito alle informazioni acquisite in

relazione alla attività economica svolta; tali informazioni devono essere aggiornate, di volta in volta, in relazione alle motivazioni economiche sottostanti alle operazioni richieste o eseguite; verifica, in occasione del censimento del cliente o del titolare effettivo e periodicamente, dell'eventuale presenza del nominativo nelle versioni aggiornate delle liste specifiche "Black list";

- Younited utilizza un sistema di screening (Dow Jones) per l'identificazione di persone politicamente esposte (PEP) e soggetti ad alto rischio
- monitoraggio nel medio-lungo periodo da parte delle Strutture operative preposte che garantisca un controllo incrociato tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione,
- l'area geografica di riferimento (con particolare riguardo all'operatività da/verso Paesi a rischio) e ancora il grado di rischio attribuito al prodotto oggetto dell'operazione, i fondi impiegati, l'orizzonte temporale dell'investimento, il comportamento tenuto dal cliente al momento dell'esecuzione dell'operazione (qualora venga eseguita in presenza del cliente);
- È previsto lo sviluppo e l'utilizzo del sistema AML Score, che consente il monitoraggio continuo e automatizzato del rischio AML della clientela.
- monitoraggio e presidio da parte delle Strutture preposte al controllo interno della puntuale esecuzione delle attività delle Strutture operative in merito alla:
  - acquisizione delle informazioni per l'identificazione e la profilatura della clientela;
  - valutazione delle operazioni rilevate dalle procedure informatiche in uso;
  - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti nella concreta operatività;
  - rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell'utilizzo del contante e dei titoli al portatore;
  - registrazione dei rapporti e delle operazioni nell'Archivio Unico Informativo ("AUI") e conservazione dei documenti e delle informazioni;
  - tutti i rapporti continuativi e le operazioni che comportano la trasmissione di mezzi di pagamento devono essere processati con modalità che consentano la registrazione procedurale nell'Archivio Unico Informatico con dati corretti e completi, anche avvalendosi di controlli automatici sulla qualità dei dati. A tale fine è indispensabile procedere alle attività di "integrazione" e "sistemazione" delle operazioni o dei rapporti in stato di "sospeso" entro i termini consentiti dalle procedure e comunque nei termini previsti dalla norma;
  - adozione di sistemi di controllo informatici atti ad impedire l'operatività riguardanti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi).
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali: al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto, in

particolare:
  - conservazione riservata e ordinata, di tutta la documentazione relativa alla identificazione e alla profilatura della clientela, ordinata per cognome nome/denominazione cliente;
  - archiviazione sistematica di tutta la documentazione relativa all'operatività e ai controlli periodici effettuati sulle posizioni relative ai clienti, presso le strutture operative di competenza;
- conservazione di traccia completa delle decisioni e delle motivazioni addotte sottostanti all'eventuale modifica del profilo del cliente e alla conseguente decisione circa l'inoltro o meno di una segnalazione di operazione sospetta alle Autorità di Vigilanza competenti.
- Riservatezza delle informazioni, con particolare riguardo a quelle relative all'individuazione dei titolari effettivi, alla profilatura dei clienti ed ai processi di monitoraggio delle operazioni e di segnalazione delle operazioni sospette, mediante l'adozione di idonee misure informatiche e fisiche.
- Formazione: è prevista la sistematica erogazione di attività specificamente dedicate alla formazione continua dei dipendenti e dei collaboratori sui profili di rischio legati alla normativa antiriciclaggio e di contrasto al finanziamento del terrorismo.

7.4.4 Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nelle attività di contrasto del riciclaggio e del finanziamento del terrorismo, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.
In particolare, le Strutture competenti sono tenute a:

- assicurare lo sviluppo e la gestione operativa delle applicazioni utilizzate nelle attività di contrasto finanziario al terrorismo/antiriciclaggio e comunque in tutte le attività che si basano sulla "adeguata conoscenza della clientela";
- verificare e garantire la diffusione all'interno delle strutture della Sede Secondaria, rispettivamente, dei provvedimenti restrittivi – contenenti limitazioni operative in specifici settori – emanate da EU, OFAC – e delle "Black list" aggiornate, nonché l'adozione di procedure automatiche di rilevazione;
- garantire che l'operatività della clientela avvenga nel rispetto dei vincoli e delle autorizzazioni previsti dalle misure di embargo ovvero dalla disciplina relativa all'esportazione di determinate categorie di merci e/o materiali (es. merce duale, sostanze chimiche pericolose);
- dettagliare nell'ambito di regolamenti/norme operative interne le regole comportamentali ad integrazione e maggiore specificazione della normativa esterna e dei principi sanciti dal presente protocollo;

- nel caso di valutazione di clientela ovvero di operazioni che interessino più strutture operative ovvero diverse società del Gruppo, collaborare tra loro e, ove consentito dalla normativa vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza del cliente e delle sue abitudini operative;
- nei rapporti instaurati con corrispondenti estere, acquisire la documentazione con cui la banca terza dichiari di adempiere agli obblighi antiriciclaggio e/o agli obblighi previsti da normative emanate da altri Stati (in particolare dagli Stati Uniti d'America);
- assicurare con continuità e sistematicità la formazione e l'addestramento del personale sulla normativa antiriciclaggio ed embarghi e sulle finalità dalle stesse perseguite;
- diffondere a tutti i collaboratori, indipendentemente dalle mansioni in concreto svolte, la normativa di riferimento ed i relativi aggiornamenti.
- Inoltre, tutti i dipendenti e collaboratori, attenendosi a quanto prescritto nelle procedure aziendali devono:
- all'atto dell'accensione di rapporti continuativi o del compimento di operazioni oltre la soglia di legge, anche se frazionate:
  - procedere all'identificazione della clientela o del titolare effettivo, e verificare dell'eventuale presenza del nominativo nelle versioni aggiornate delle "Black List";
  - verificare la sussistenza di eventuali titolari effettivi, acquisire informazioni sullo scopo e sulla natura del rapporto o dell'operazione e, qualora il cliente sia una società o un Ente, verificare la sussistenza dei poteri di rappresentanza e la struttura di proprietà e di controllo del cliente;
  - procedere alla profilatura della clientela;
- mantenere aggiornati tutti i dati relativi ai rapporti continuativi al fine di consentire una costante valutazione del profilo economico e finanziario del cliente;
- effettuare l'adeguata verifica e la profilatura della clientela quando, indipendentemente da qualsiasi soglia di importo o di esenzione applicabile, vi sia il sospetto di riciclaggio, dì finanziamento del terrorismo o sorgano dubbi sulla veridicità o sull'adeguatezza dei dati identificativi già acquisiti;
- mantenere l'assoluto riserbo sulle informazioni relative alla fascia di rischio antiriciclaggio attribuita al cliente e al relativo punteggio calcolato dalla procedura, che in nessun caso devono essere comunicati alla clientela;
- collaborare attivamente ai processi per la rilevazione e la segnalazione delle operazioni sospette;
- valutare se dare l'avvio all'iter di segnalazione in presenza di indici di anomalia anche se non rilevati dalle procedure informatiche, o nei casi in cui risulti impossibile rispettare gli obblighi di adeguata verifica;
- verificare l'eventuale censimento dei clienti o dei titolari effettivi nelle versioni aggiornate delle Black List e bloccare o, comunque, non dare esecuzione ad operazioni che vedano coinvolti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti

transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi) o per le quali sussista comunque il sospetto di una relazione con il riciclaggio o con il finanziamento del terrorismo;

- inoltrare le comunicazioni delle infrazioni delle disposizioni in tema di limitazioni all'uso del contante e dei titoli al portatore rilevabili nell'operatività della clientela;
- rispettare rigorosamente le procedure interne in tema di registrazione dei rapporti e delle operazioni in AUI e di conservazione della documentazione.

Tutti i dipendenti della Sede Secondaria, senza distinzioni di rapporto giuridico in base al quale sono legati a Younited incaricati di attività valutative o autorizzative previste dai processi in materia di antiriciclaggio, devono esercitare la discrezionalità loro rimessa secondo criteri di professionalità e ragionevolezza. In caso di conflitti di interesse, anche potenziali, di ordine personale o aziendale devono:

- informare immediatamente il proprio superiore gerarchico della sussistenza del conflitto di interessi precisandone la natura, i termini, l'origine e la portata;
- astenersi dall'attività valutativa / autorizzativa, rimettendo la decisione al proprio superiore gerarchico o alla Struttura specificamente individuata nella normativa interna per l'evenienza. A titolo esemplificativo, possono ricorrere situazioni di conflitto di interessi qualora l'interesse personale interferisca (o appaia interferire) con l'interesse della Sede Secondaria o del Gruppo, impedendo l'adempimento obiettivo ed efficace delle proprie funzioni, ovvero in relazione al perseguimento di benefici personali impropri come conseguenza della posizione ricoperta in seno alla Sede Secondaria o al Gruppo.

È inoltre fatto divieto comunicare, anche in modo involontario, a terzi (inclusi i soggetti con i quali sussistono rapporti di familiarità diretta o stretti legami propri o dei propri congiunti) per ragioni diverse da quelle di ufficio, il contenuto delle attività valutative / autorizzative al di fuori dei casi previsti dalla legge.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001 e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- instaurare rapporti continuativi, o mantenere in essere quelli preesistenti, ed eseguire operazioni quando non è possibile attuare gli obblighi di adeguata verifica nei confronti del cliente, ad esempio per il rifiuto del cliente a fornire le informazioni richieste;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio, con il finanziamento del terrorismo;
- ricevere od occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;
- sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero

compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
- partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione;
- mettere a disposizione di clientela appartenente o comunque contigua alla malavita organizzata servizi, risorse finanziarie o disponibilità economiche che risultino strumentali al perseguimento di attività illecite.

7.5. Gestione dei conti correnti e delle carte di pagamento

7.5.1 Premessa

La gestione dei conti correnti e delle carte di pagamento della Sede Secondaria di Younited rientra tra le attività sensibili ai fini del D.Lgs. 231/2001, in relazione ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio, nonché ai delitti in materia di strumenti di pagamento diversi dai contanti.
L'attività è svolta in conformità alle policy di Gruppo e alle procedure locali, con l'obiettivo di prevenire e contrastare l'utilizzo improprio di mezzi di pagamento aziendali e la realizzazione di operazioni che possano, anche indirettamente, agevolare condotte illecite.

7.5.2 Descrizione del processo

La gestione dei conti correnti e delle carte di pagamento si articola nelle seguenti attività:
- Le carte di pagamento utilizzate dalla Sede Secondaria sono esclusivamente virtuali e temporanee, generate per singola transazione e automaticamente estinte dopo l'utilizzo.
- Il processo di gestione delle note spese è effettuato tramite un workflow digitale, con:
  - controlli automatici di soglia;
  - approvazione multilivello;
  - verifica ex ante da parte del manager responsabile e del team HR.
- È previsto un campionamento trimestrale da parte del controllo interno sulle spese effettuate.
- Gli eventuali alert o anomalie rilevate dal sistema contabile sono gestiti dal Finance Operations, che informa tempestivamente l'Organismo di Vigilanza.

7.5.3 Principi di controllo

I principali controlli attivi sul processo sono:
- Emissione di carte virtuali e temporanee per singola transazione, al fine di limitare il rischio di utilizzo improprio o frode.

- Controlli automatici di soglia sulle spese, integrati nel sistema digitale di gestione.
- Approvazione multilivello delle note spese, con verifica preventiva da parte del manager e del team HR.
- Campionamento trimestrale delle spese da parte del controllo interno, per verifica di conformità.
- Gestione degli eventuali alert generati dal sistema contabile a cura del Finance Operations, con segnalazione all'OdV.
- Non sono previsti sistemi antifrode dedicati, in quanto il rischio residuo è stato valutato "irrilevante".

7.5.4 Principi di comportamento

Tutti i soggetti coinvolti nella gestione dei conti correnti e delle carte di pagamento devono:

- utilizzare le carte aziendali esclusivamente per spese legittime e autorizzate;
- garantire la corretta compilazione e registrazione delle note spese, attenendosi al workflow previsto;
- segnalare tempestivamente eventuali anomalie o comportamenti sospetti al proprio responsabile;
- cooperare pienamente con le attività di controllo interno e con le verifiche trimestrali previste;
- evitare qualsiasi comportamento che possa integrare una delle fattispecie di reato previste dal D.Lgs. 231/2001 in materia di riciclaggio, autoriciclaggio o uso illecito di strumenti di pagamento.

Reati di terrorismo ed eversione dell'ordine democratico – art. 25-*quater* D.Lgs. 231/2001

La Sede Secondaria si è dotata di presidi specifici finalizzati a prevenire la commissione, anche indiretta, di reati di terrorismo o aventi finalità eversive, nonché di delitti connessi all'uso illecito di esplosivi o armi, così come previsto e aggiornato dall'art. 25-quater del Decreto.
In particolare:

- Nel processo di assunzione e onboarding dei dipendenti, è stato introdotto un sistema di verifica preventiva (name screening), tramite confronto con liste ufficiali per intercettare eventuali soggetti legati, direttamente o indirettamente, ad attività di terrorismo internazionale, eversione o traffico illecito di esplosivi/armi.
- Il processo di onboarding include la raccolta e la verifica della documentazione identificativa, nonché la sottoscrizione di dichiarazioni circa l'assenza di condanne o procedimenti in corso per reati contro la sicurezza pubblica e l'ordine democratico.
- Analoghi controlli di name screening e verifica reputazionale sono effettuati anche nei confronti di fornitori, consulenti, collaboratori e soggetti terzi, prima

dell'avvio di qualsiasi rapporto contrattuale.

- La Funzione Compliance e/o Antiriciclaggio, in coordinamento con l'Organismo di Vigilanza, assicura il monitoraggio periodico delle liste sanzionatorie, integrando i controlli in caso di aggiornamenti normativi o nuove segnalazioni da fonti istituzionali.

Tali misure sono parte integrante del sistema di prevenzione dei rischi 231 e sono finalizzate a impedire che l'organizzazione possa essere utilizzata, anche inconsapevolmente, come canale o piattaforma per il supporto a condotte illecite di matrice terroristica o eversiva.

7.6. Flussi informativi all'Organismo di Vigilanza

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.
- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua verifiche ad evento, semestrali ed annuali**.**

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Funzione Antiriciclaggio (AML)	Relazione annuale AML con sintesi delle attività svolte, criticità emerse e follow-up	Annuale
Responsabile Succursale	Segnalazioni di operazioni Sospette, con notifica all'OdV	Ad evento
Funzione Antiriciclaggio (AML)	Relazione di Attestazione Annuale ex Provvedimento Banca d'Italia	Annuale
Funzione Antiriciclaggio (AML)	Report semestrale sul monitoraggio clienti, operazioni anomale, presidi attivati	Semestrale
Dipartimento Finance Operations	Comunicazione anomalie rilevate sull'uso delle carte di pagamento o spese sospette	Ad evento

8.REATO DI IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (ART. 25-DUODECIES)

8.1. Le fattispecie di reato previste dall'art. 25-*duodecies* del Decreto

L'articolo 25-duodecies del D.Lgs. 231/2001, introdotto con il D.Lgs. 109/2012, ha esteso il catalogo dei reati presupposto alla responsabilità amministrativa degli enti, includendo i reati in materia di immigrazione, con particolare riferimento all'impiego di lavoratori stranieri il cui soggiorno in Italia sia irregolare.

Il reato si configura qualora un datore di lavoro occupi alle proprie dipendenze uno o più cittadini stranieri privi del permesso di soggiorno o con permesso scaduto, revocato o annullato, nei casi previsti dalla norma.
Introdotto con D.Lgs. 16 luglio 2012, n. 109, l'articolo prevede che:
L'ente è responsabile se, nell'interesse o a vantaggio dell'ente stesso, viene commesso il reato previsto dall'articolo 22, comma 12-bis, del D.Lgs. 286/1998 (Testo Unico sull'Immigrazione), ovvero: "L'impiego di lavoratori stranieri privi del permesso di soggiorno".

L'art. 25-duodecies del D.Lgs. 231/2001 è stato modificato dalla Legge 161/2017 che ha esteso il novero dei reati presupposto richiamando l'art. 12 del D.Lgs. 286/1998 ("Disposizioni contro le immigrazioni clandestine"), con riferimento ai soli commi 3, 3-bis, 3-ter e 5, di seguito riportati:

- Comma 3: Salvo che il fatto costituisca più grave reato, chiunque, in violazione delle disposizioni del presente testo unico, promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente, nel caso in cui: a) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone; b) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale; c) la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale; d) il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti; e) gli autori del fatto hanno la disponibilità di armi o materie esplodenti.

- Comma 3 bis. Se i fatti di cui al comma 3 sono commessi ricorrendo due o più delle ipotesi di cui alle lettere a), b), c), d) ed e) del medesimo comma, la pena ivi prevista è aumentata.

- Comma 3 ter. La pena detentiva è aumentata se i fatti di cui ai commi 1 e 3: a) sono commessi al fine di reclutare persone da destinare alla prostituzione o comunque allo sfruttamento sessuale o lavorativo ovvero riguardano l'ingresso di minori da impiegare in attività illecite al fine di favorirne lo sfruttamento; b) sono commessi al fine di trame profitto, anche indiretto.

- Comma 5. Fuori dei casi previsti dai commi precedenti, e salvo che il fatto non costituisca più grave reato, chiunque, al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero o nell'ambito delle attività punite a norma del presente articolo, favorisce la permanenza di questi nel territorio dello Stato in violazione delle norme del presente testo unico. Quando il fatto è commesso in concorso da due o più persone, ovvero riguarda la permanenza di cinque o più persone, la pena è aumentata da un terzo alla metà.

8.2. Le Attività Aziendali sensibili

Ad oggi, non sono emerse criticità relativamente alla Sede Secondaria.
Le attività ritenute sensibili ai fini della prevenzione del reato di impiego di lavoratori stranieri irregolari sono le seguenti:

- Gestione delle assunzioni e verifica della documentazione identificativa e autorizzativa (es. permesso di soggiorno, titolo di soggiorno valido per lavoro).
- Gestione dei contratti di lavoro subordinato e delle prestazioni occasionali o temporanee, anche tramite agenzie.
- Gestione degli appalti e delle forniture, con particolare attenzione alle imprese esterne che forniscono personale (es. servizi di pulizia, manutenzione, logistica o altri servizi generici).

8.3. Descrizione del Processo

La Società ha individuato specifiche attività sensibili al rischio di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, in particolare con riferimento alla gestione del personale e dei rapporti con fornitori di manodopera.
Il processo di gestione del rischio si articola come segue:

1. Raccolta e verifica della documentazione anagrafica e di soggiorno

In fase di assunzione di personale extra-UE, la funzione HR è tenuta a:

- acquisire copia del documento d'identità e del titolo di soggiorno (permesso o altro documento valido);
- verificare la validità del titolo di soggiorno e la coerenza con il tipo di contratto proposto (es. lavoro subordinato, stage, collaborazione, prestazione occasionale).

La documentazione raccolta viene archiviata nel fascicolo del dipendente, in formato digitale o cartaceo, accessibile solo al personale autorizzato.

2. Gestione degli appalti e verifica dei fornitori

Le strutture aziendali preposte sono tenute a verificare, in fase di stipula o rinnovo contrattuale, che le imprese appaltatrici:

- dichiarino il rispetto della normativa in materia di impiego di manodopera regolare, anche straniera;
- presentino un **DURC** in corso di validità;
- sottoscrivano clausole contrattuali che prevedano:
  - l'obbligo di comunicazione preventiva in caso di subappalto o sostituzione del personale;
  - il rispetto delle disposizioni legislative in materia di immigrazione.

8.4. Principi di controllo

Il sistema di controllo a presidio del processo di gestione delle attività a rischio connesse al reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare deve garantire l'effettività dei presidi previsti, sulla base dei seguenti elementi:

Livelli autorizzativi definiti nell'ambito del processo

Il sistema di gestione delle risorse umane prevede la definizione di responsabilità chiare e formalizzate per ciascuna fase del processo di:

- selezione,
- assunzione,
- verifica della documentazione anagrafica e amministrativa.

Segregazione dei compiti

È assicurata la separazione funzionale tra:

- chi effettua il reclutamento e la selezione del personale,
- chi è incaricato della verifica della documentazione identificativa e di soggiorno,
- chi gestisce la formalizzazione del rapporto di lavoro e la trasmissione dei dati agli enti preposti (INPS, INAIL, Centro per l'Impiego, Questura).

Tale separazione garantisce un controllo incrociato e riduce il rischio di omissioni o abusi.

8.5. Attività di controllo

Le strutture competenti devono attuare un piano di controlli periodici finalizzato a:

- verificare la correttezza e completezza della documentazione acquisita in fase di assunzione, con particolare riferimento ai cittadini extra-UE;
- monitorare la validità nel tempo dei titoli di soggiorno, con aggiornamento dei fascicoli e segnalazione automatica delle scadenze;
- esaminare, tramite audit interni, la conformità dei fornitori e appaltatori alle normative in materia di lavoro e immigrazione, anche attraverso l'acquisizione della dichiarazione di regolarità e l'accesso ai DURC e alle autocertificazioni;
- aggiornare i modelli contrattuali con apposite clausole 231 in tema di rispetto

della normativa sull'immigrazione, responsabilità solidale e obbligo di comunicazione in caso di subappalto.

8.6. Tracciabilità del processo

Tutte le fasi del processo devono essere tracciabili e documentate, nel rispetto della normativa vigente:

- le strutture coinvolte devono archiviare in formato cartaceo o elettronico la documentazione relativa a permessi di soggiorno, contratti e dichiarazioni del lavoratore;
- la documentazione è custodita in appositi fascicoli digitali, accessibili solo a personale autorizzato, secondo criteri di riservatezza e protezione dei dati;
- il sistema informativo HR deve prevedere alert automatici per le scadenze dei titoli di soggiorno;
- per i contratti in appalto, la struttura preposta deve conservare le dichiarazioni di conformità e verificare, tramite check list, la presenza di clausole contrattuali specifiche.

8.7. Principi di comportamento

Tutti i soggetti coinvolti nella gestione delle attività sopra descritte devono:

- Verificare, prima dell'instaurazione del rapporto di lavoro, la validità del permesso di soggiorno o di altro titolo che abiliti alla permanenza e all'impiego in Italia.
- Astenersi dall'instaurare o mantenere rapporti di lavoro con cittadini extracomunitari in posizione di irregolarità sul territorio nazionale.
- Garantire che, per ogni assunzione, sia acquisita e conservata la documentazione relativa alla regolarità del soggiorno e al permesso di lavoro.
- In caso di contratti di appalto o fornitura, verificare che le imprese appaltatrici rispettino gli obblighi normativi in materia di lavoro e immigrazione, anche mediante clausole contrattuali specifiche.

8.8. Flussi informativi all'Organismo di Vigilanza

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica

eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.

- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua verifiche ad evento, semestrali e annuali.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	**Descrizione del flusso informativo**	**Periodicità**
HR	Segnalazione di assunzione di lavoratori extra-UE	Ad evento
HR	Notifica di documentazione mancante o irregolare sul titolo di soggiorno	Ad evento
HR	Report semestrale su verifiche documentali e permessi di soggiorno validi	semestrale
HR	Comunicazione di nuovi appalti o modifiche contrattuali con imprese fornitrici di personale	Ad evento
HR	Dichiarazioni di conformità/acquisizione DURC e clausole 231 nei contratti d'appalto	Ad evento

9. REATI DI ABUSO DI MERCATO

Si descrivono di seguito le singole fattispecie di reato e di illecito amministrativo per le quali l'art. 25-sexies, D.Lgs. 231/2001 e l'art. 187-quinquies D.Lgs. n. 58/98 (di seguito, "TUF") prevedono la responsabilità della Società nei casi in cui tali reati e illeciti amministrativi siano stati compiuti nell'interesse o a vantaggio della società stessa.

La definizione di "informazione privilegiata"

Attorno al concetto di informazione privilegiata ruota l'intera disciplina sull'insider trading e quella concernente l'informazione societaria disciplinata nel Titolo III, Capo I, artt. 114 e seguenti del TUF e nel Regolamento Emittenti n. 11971/1999. Secondo quanto previsto dall'art. 180, lett. b-ter, TUF, si intendono di carattere privilegiato le informazioni che presentano le seguenti caratteristiche (qui di seguito le "**Informazioni Privilegiate**"):

a. sono di carattere preciso e pertanto:

i) devono essere inerenti a un complesso di circostanze o eventi esistenti

o verificatisi o a circostanze o eventi che ragionevolmente possa prevedersi che verranno ad esistenza o che si verificheranno (il riferimento è ai casi in cui la notizia è in via di formazione e riguarda eventi non ancora verificatisi, si pensi al caso caratterizzato dalla notizia che una società quotata stia per lanciare un'OPA, oppure il caso riguardante un piano strategico di riposizionamento produttivo della società emittente i titoli); e

ii) devono essere sufficientemente specifiche (ossia esplicite e dettagliate), in modo che chi le impiega sia posto in condizione di ritenere che dall'uso delle stesse potranno effettivamente realizzarsi quegli effetti sul prezzo degli strumenti finanziari;

b. non sono ancora state rese pubbliche;

c. riguardano, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, e sono relative alla situazione economica patrimoniale ("corporate information") ovvero a vicende organizzative dell'emittente ("market information");

d. sono "price sensitive", ossia sono tali che, se rese pubbliche, sarebbero presumibilmente utilizzate da un investitore ragionevole come uno degli elementi su cui fondare le proprie decisioni di investimento.

Con riferimento alla definizione in oggetto si elencano qui di seguito, a mero titolo esemplificativo e non esaustivo, alcune circostanze in cui la Società potrebbe trovarsi a dover gestire Informazioni Privilegiate appartenenti ad altre società: - distribuzione di prodotti assicurativi a prevalente contenuto finanziario; - dati revisionali e obiettivi quantitativi concernenti l'andamento della gestione; - comunicazioni relative a operazioni di fusione/scissione e a nuove iniziative di particolare rilievo ovvero a trattative e/o accordi in merito all'acquisizione e/o cessione di asset significativi; - attività di finanza straordinaria, quali, a titolo esemplificativo, fusioni, scissioni, incorporazioni, scorpori; - mutamento nel controllo o nei patti parasociali di controllo; - cambiamenti nell'organo di amministrazione e controllo; - modifica del revisore o qualsiasi informazione collegata alla sua attività; operazioni sul capitale o emissione di obbligazioni o warrant per acquistare/sottoscrivere azioni; - aumento o diminuzione del capitale sociale; - acquisto o cessione di partecipazioni o altri asset o attività rilevanti; - ristrutturazione o riorganizzazione che abbiano un effetto sul bilancio; - decisioni relative ai programmi di acquisto di azioni proprie o operazioni aventi ad oggetto altri strumenti finanziari quotati; - modifiche dei diritti relativi a determinate categorie di azioni quotate; - istanze di fallimento ovvero ordinanze del tribunale relative a procedure concorsuali; - significative controversie legali; - revoca o cancellazione di linee di credito; - liquidazione volontaria o altre cause di liquidazione; - rilevante cambiamento nel valore degli asset; - insolvenza dei principali debitori;

9.1. Le fattispecie di reato previste dal Decreto

Abuso o comunicazione illecita di informazioni privilegiate. raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (Art.184 TUF)

La disposizione di cui all'art. 184 del TUF punisce chiunque, essendo in

possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero l'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

- acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
- comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del MAR5 ;
- raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

La stessa disposizione si applica a chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni appena menzionate, nonché al c.d. "insider secondario", ovvero a colui che compie le operazioni di cui sopra sfruttando informazioni privilegiate ottenute anche al di fuori della propria attività lavorativa. Si applica la sanzione penale anche nel caso in cui le operazioni riguardino gli strumenti finanziari di cui all'articolo 180, co. 1, lettera a), numeri 2), 2-bis) e 2-ter)6 del TUF, limitatamente agli strumenti finanziari il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario di cui ai numeri 2) e 2-bis) ovvero ha un effetto su tale prezzo o valore, o relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni.

Manipolazione di mercato (Art.185 TUF)
La fattispecie punisce chiunque diffonde notizie false (c.d. manipolazione informativa) o pone in essere operazioni simulate o altri artifizi (c.d. manipolazione operativa) concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

Si ha manipolazione informativa anche allorquando la creazione di un'indicazione fuorviante derivi dall'inosservanza degli obblighi di comunicazione da parte dell'emittente o di altri soggetti obbligati.

La disposizione di cui all'art. 185 del TUF punisce chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari. Tuttavia, non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del MAR.

Ai sensi dell'art. 182 TUF, si applica la sanzione penale anche nel caso in cui le operazioni sono relative agli strumenti finanziari di cui all'articolo 180, co. 1, lettera a), numeri 2), 2- bis) e 2-ter), limitatamente agli strumenti finanziari il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario di cui ai numeri 2) e 2-bis) ovvero ha un effetto su tale prezzo o valore, o relative

alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni. Sempre ai sensi dell'art. 182 TUF, le disposizioni summenzionate si applicano anche:

- ai fatti concernenti i contratti a pronti su merci che non sono prodotti energetici all'ingrosso, idonei a provocare una sensibile alterazione del prezzo o del valore degli strumenti finanziari di cui all'articolo 180, co. 1, lettera a);
- ai fatti concernenti gli strumenti finanziari, compresi i contratti derivati o gli strumenti derivati per il trasferimento del rischio di credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronti su merci, qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari;
- ai fatti concernenti gli indici di riferimento (benchmark).

Gli illeciti amministrativi ex art. 187-*quinquies* del TUF

L'art. 187-quinquies del TUF opera un rinvio espresso alla normativa europea, disponendo, in particolare, che siano vietate le condotte che violino l'art. 14 o l'art. 15 del Regolamento MAR – Market Abuse Regulation, UE 596/2014.

Abuso di informazioni privilegiate e comunicazione illecita di informazioni privilegiate (Art.14 Regolamento Mar)

L'art. 14 del Regolamento MAR prevede che non sia consentito:

a) abusare o tentare di abusare di informazioni privilegiate;
b) raccomandare ad altri di abusare di informazioni privilegiate o indurre altri ad abusare di informazioni privilegiate; oppure
c) comunicare in modo illecito informazioni privilegiate.

I comportamenti degli insider secondari sono puniti sia se sono commessi a titolo di dolo sia se sono commessi con colpa.

Le definizioni dei divieti in questione sono contenute in particolare negli articoli 8 (abuso di informazioni privilegiate) e 10 (comunicazione illecita di informazioni privilegiate) del MAR.

Divieto di manipolazione del mercato (Art. 15 Regolamento Mar)

In base all'art. 15 del MAR, non è consentito effettuare manipolazioni di mercato o tentare di effettuare manipolazioni di mercato.

Le definizioni relative al divieto in questione sono contenute in particolare nell'art. 12 (manipolazione del mercato) del MAR.

Ai sensi dell'art. 12 del MAR, per manipolazione del mercato si intendono le seguenti attività:

a. la conclusione di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra condotta che:
   i. invii, o è probabile che invii, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni;
   ii. fissi, o è probabile che fissi, il prezzo di mercato di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale o artificiale; a meno che la persona che avvia un'operazione, inoltra un ordine di

compravendita o ha posto in essere qualsiasi altra condotta dimostri che tale operazione, ordine o condotta sono giustificati da legittimi motivi e sono conformi a una prassi di mercato ammessa, come stabilito a norma dell'articolo 13 del MAR;

b. la conclusione di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra attività o condotta che incida, o sia probabile che incida, sul prezzo di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni, utilizzando artifici o qualsiasi altra forma di raggiro o espediente;
c. la diffusione di informazioni tramite i mezzi di informazione, compreso Internet, o tramite ogni altro mezzo, che forniscano, o siano idonee a fornire, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni o che consentano, o è probabile che consentano, di fissare il prezzo di mercato di uno o più strumenti finanziari o di contratti a pronti su merci collegati o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale o artificiale, compresa la diffusione di voci, quando la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti;
d. la trasmissione di informazioni false o fuorvianti o la comunicazione di dati falsi o fuorvianti in relazione a un indice di riferimento (benchmark) quando la persona che ha proceduto alla trasmissione o fornito i dati sapeva, o avrebbe dovuto sapere, che erano falsi o fuorvianti, ovvero qualsiasi altra condotta che manipola il calcolo di un indice di riferimento.

9.2. Le Attività Aziendali sensibili

In considerazione della quotazione della capogruppo Younited Financial S.A. sui mercati regolamentati Euronext di Parigi e Amsterdam, nonché dell'operatività della Sede Secondaria italiana, quale banca francese operante in Italia, risultano rilevanti, ai sensi del D.Lgs. 231/2001, alcune fattispecie di reato di natura finanziaria e societaria connesse allo status di società emittente strumenti finanziari quotati.
Sono considerate particolarmente esposte al rischio di commissione di tali reati le seguenti attività aziendali sensibili:

- Predisposizione, approvazione e diffusione di bilanci e relazioni finanziarie, nonché comunicazioni sociali e documenti contabili;
- Gestione delle informazioni privilegiate e price sensitive, con accesso a sistemi informativi contenenti dati finanziari rilevanti;
- Rapporti con autorità di vigilanza nazionali e straniere (Consob, Banca d'Italia, AMF, AFM) e con i mercati regolamentati;
- Redazione e pubblicazione di prospetti, documenti informativi e comunicazioni al pubblico;
- Gestione delle operazioni con parti correlate e delle operazioni straordinarie;
- Attività di audit, compliance e risk management su processi finanziari e societari.

9.3. Descrizione del Processo

La Società ha individuato specifiche attività sensibili e ha adottato, mantenendole in vigore, le seguenti procedure:
- **Market Abuse Policy** di Younited;
- **Insider Trading Procedure** di Younited;
- **Related Party Transactions Policy** di Younited Financial;
- **Disclosure Policy** di Younited Financial.

Tali procedure definiscono criteri, ruoli e responsabilità per:
- la gestione delle informazioni privilegiate;
- la comunicazione al mercato;
- la corretta tenuta dei documenti societari;
- la prevenzione di fenomeni di market abuse.

9.4. Misure attualmente adottate dalla Società

A titolo esemplificativo e non esaustivo, si riportano di seguito le principali misure già concretamente implementate dalla Società, a presidio dei rischi connessi ai reati di abuso di mercato, in applicazione dei principi sopra indicati:

Comunicazioni e responsabilizzazione dei dipendenti
- Informativa periodica ai dipendenti circa le limitazioni operative sui titoli, con specifica indicazione dei periodi di divieto;
- Obbligo per i dipendenti di informare preventivamente la Funzione Compliance in caso di operazioni rilevanti;
- Erogazione di training dedicato al top management, con successiva diffusione delle policy e delle procedure interne;
- Programmazione di iniziative formative estese a tutti i dipendenti di Younited e delle succursali, inclusa quella italiana, con focus specifico in materia di abusi di mercato;
- Monitoraggio accentrato da parte della Funzione Compliance della capogruppo;
- Comunicazioni periodiche ai dipendenti in occasione di eventi societari sensibili (ad esempio, approvazione della semestrale).

Audit e verifiche periodiche
- Svolgimento di attività di audit interno e di compliance finalizzate a verificare l'aderenza alle procedure e l'efficacia dei controlli;
- Reporting periodico agli organi di governance in merito a eventuali criticità riscontrate.

9.5. Gestione delle operazioni con parti correlate e delle operazioni straordinarie

- Controlli preventivi e documentati sulle operazioni con parti correlate;
- Adozione di procedure specifiche per l'approvazione e la comunicazione di operazioni straordinarie, in conformità con le policy interne e le disposizioni normative applicabili.

Tracciamento e conservazione documentale
- Archiviazione sicura di tutta la documentazione rilevante (documenti contabili, bilanci, comunicazioni societarie, prospetti, ecc.);
- Adozione di misure idonee a garantire l'integrità, la riservatezza e la disponibilità dei dati, al fine di consentire eventuali verifiche interne ed esterne.

9.6. Principi di controllo

Il sistema di controllo a presidio delle **attività sensibili** deve garantire l'effettività dei presidi previsti, basandosi sui seguenti elementi:

1. **Segregazione delle funzioni**
   - Chiarezza dei ruoli e delle responsabilità nelle attività sensibili;
   - Separazione tra chi genera informazioni privilegiate e chi le utilizza o comunica al mercato.
2. **Registri degli insider**
   - Tenuta di liste aggiornate delle persone con accesso a informazioni privilegiate;
   - Aggiornamento periodico dei registri e comunicazione agli organi di vigilanza quando richiesto.
3. **Autorizzazioni e procedure di approvazione**
   - Procedure interne per approvare la diffusione di comunicazioni finanziarie, prospetti, relazioni periodiche e operazioni straordinarie;
   - Autorizzazioni multiple per le decisioni strategiche e operative a rischio di abuso di mercato.
4. **Controlli di comunicazione e disclosure**
   - Validazione e controllo preventivo di comunicazioni al mercato e rapporti con investitori;
   - Tracciamento delle informazioni divulgate per garantire trasparenza e correttezza.
5. **Monitoraggio delle operazioni sui titoli**
   - Controllo delle transazioni su strumenti finanziari della società da parte di insider o soggetti rilevanti;
   - Segnalazione tempestiva di eventuali operazioni sospette alle funzioni di compliance.
6. **Formazione e sensibilizzazione**
   - Programmi periodici di formazione su insider trading, market abuse e gestione di informazioni privilegiate per tutte le persone con accesso ad attività sensibili;
   - Aggiornamento continuo rispetto a normativa nazionale e regolamentazioni UE.

9.7. Principi di comportamento

Tutti i soggetti coinvolti devono:

- assicurare la veridicità, completezza e tempestività delle comunicazioni sociali e finanziarie;
- mantenere riservate le informazioni privilegiate fino a comunicazione ufficiale al mercato;
- rispettare i divieti di insider trading e di manipolazione del mercato;
- astenersi da comportamenti che possano impedire o ostacolare le funzioni di controllo;
- segnalare tempestivamente all'OdV eventuali anomalie o violazioni.

9.8. I Flussi informativi all'Organismo di Vigilanza

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue.
Le funzioni aziendali comunicano all'OdV:

- ogni violazione o sospetto di violazione della Market Abuse Policy o della Insider Trading Procedure;
- relazioni periodiche su disclosure e comunicazioni al mercato;
- esiti degli audit interni su processi di bilancio, disclosure e gestione delle informazioni privilegiate;
- segnalazioni su anomalie o sospetti di manipolazione del mercato o abuso di informazioni privilegiate.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	**Flusso Informativo**	**Periodicità**
Compliance/Legal	Comunicazioni ad hoc su violazioni Market Abuse o Insider Trading	Ad evento
Investor Relations	Relazioni periodiche su disclosure e comunicazioni al mercato	Semestrale/annuale
Internal Audit	Esiti audit su processi di bilancio, disclosure e gestione informazioni privilegiate	Annuale
Tutte le Funzioni	Segnalazioni su anomalie o sospetti di manipolazione mercato o abuso di informazioni privilegiate	Ad evento

10. REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

10.1. Premessa

La presente Parte Speciale ha l'obiettivo di illustrare i criteri, i ruoli e le responsabilità, i principi di controllo e le regole di comportamento cui tutti i destinatari del Modello, ivi compresi i Consulenti, il personale, i fornitori e i

partner, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dagli articoli 25-*septies* del Decreto , nel rispetto dei principi di legalità, correttezza, oggettività, trasparenza, tracciabilità e riservatezza nell'esecuzione delle proprie attività, della normativa emanata dagli organismi di vigilanza e di tutte le leggi e le norme nazionali ed internazionali vigenti.

10.2. Le fattispecie di reato previste dall'art. 25-*septies* del Decreto

L'art. 25-*septies* del Decreto prevede tra gli illeciti presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.
Il Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro, (D. Lgs, 9 aprile 2008 n. 81) che ha profondamente riordinato le molteplici fonti normative previgenti in materia. con l'art. 30 ha esplicitato le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.
Finalità delle citate disposizioni è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione alla recrudescenza del fenomeno degli incidenti sul lavoro ed alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.
Si fornisce qui di seguito una sintetica descrizione dei reati sopra menzionati.
Omicidio colposo (art. 589 c.p.) Il reato si configura ogni qualvolta un soggetto cagioni per colpa la morte di altro soggetto.
Nel contesto aziendale, la responsabilità può insorgere in presenza di violazioni degli obblighi previsti dalla normativa in materia di salute e sicurezza sul lavoro, qualora non vengano adottate misure adeguate a prevenire eventi lesivi nei confronti di lavoratori o di soggetti terzi.
Il reato di omicidio colposo rileva ai fini del D.Lgs. 231/2001 se commesso in violazione della normativa antinfortunistica e della tutela della salute e sicurezza sul lavoro, costituendo reato presupposto ai sensi dell'art. 25-septies del Decreto.

Lesioni personali colpose gravi o gravissime (art. 590 comma 3 c.p.) Le condotte punite dalle due fattispecie consistono nel cagionare per colpa, rispettivamente, la morte oppure una lesione dalla quale deriva una malattia, nel corpo o nella mente, grave o gravissima.
Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso. Ai sensi del predetto art. 25-septies del Decreto, entrambe le condotte devono essere caratterizzate dalla violazione delle norme dettate ai fini della prevenzione degli infortuni sul lavoro e sulla tutela dell'igiene e della salute sul lavoro.
Vengono a tal proposito in considerazione molteplici disposizioni, ora in gran parte confluite nel Testo Unico in materia di tutela della salute e della sicurezza

nei luoghi di lavoro a seguito dell'abrogazione da parte del medesimo Testo Unico di varie leggi speciali previgenti, tra le quali, fondamentalmente: il D.P.R. 27.4.1955 n. 547 in tema di prevenzione degli infortuni; il D.P.R. 19.3.1956 n. 303 sull'igiene del lavoro; il D. Lgs. 19.9.1994
n. 626 che conteneva norme generali sula tutela della salute e della sicurezza dei lavoratori; il D. Lgs. 14.8.1996 n. 494 in tema di sicurezza dei cantieri.
A completamento del corpo normativo delineato dalle specifiche misure di prevenzione prescritte dalle leggi in materia si colloca la più generale previsione di cui all'art. 2087 del codice civile, in forza del quale il datore di lavoro deve adottare le misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie per tutelare l'integrità fisica e morale dei lavoratori.
Va infine tenuto presente che la giurisprudenza ritiene che i reati in questione siano imputabili al datore di lavoro anche qualora la persona offesa non sia un lavoratore, ma un estraneo, purché la sua presenza sul luogo di lavoro al momento dell'infortunio non abbia caratteri di anormalità ed eccezionalità.

10.3. Le Attività Aziendali sensibili

Le attività sensibili sono:

- Gestione dei rischi in materia di salute e sicurezza sul lavoro anche con riferimento all'attività svolta da appaltatori e subappaltatori
- Gestione del lavoro agile (smart working)
- Gestione dell'accesso ai clienti e terzi agli spazi aziendali

Si riportano di seguito i protocolli che dettano i principi di controllo e i principi di comportamento applicabili.

Tali protocolli si completano con la normativa aziendale di dettaglio vigente in argomento.
Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio dalle altre società del Gruppo e/o *outsourcer* esterni.

10.4. Gestione dei rischi in materia di salute e sicurezza sul lavoro anche con riferimento all'attività svolta da appaltatori e subappaltatori

10.4.1 Premessa

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D. Lgs. n.81/2008 (di seguito Testo Unico).
Si rammenta anzitutto che, ai sensi del Testo Unico compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e compete al Committente e/o ai suoi delegati la responsabilità e la gestione dei cantieri temporanei o mobili disciplinati dal Titolo IV del Testo Unico nonché compete ad entrambi, per gli ambiti di rispettiva pertinenza, il rispetto degli obblighi relativi all'affidamento di

contratti d'appalto, d'opera o di somministrazione previsti dall'art. 26 del medesimo Testo Unico.
In ottemperanza a quanto disposto dalla predetta normativa, la Sede Secondaria ha adottato un sistema di gestione della salute e sicurezza sul lavoro in conformità al D.Lgs. 81/2008 e al D.Lgs. 231/2001, affidando le attività di supporto a un Responsabile del Servizio di Prevenzione e Protezione (RSPP) esterno, inoltre ha adottato e tiene aggiornato il "*Documento di Valutazione dei Rischi*" (DVR), che contiene:

- la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;
- l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori ed il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, dei rappresentanti dei lavoratori per la sicurezza e dei medici competenti che hanno partecipato alla valutazione del rischio;
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

La Società ha in essere due contratti continuativi con imprese appaltatrici:

- Ditta di pulizie
- Ditta di manutenzione

Per l'impresa di pulizie è stato predisposto il Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI), aggiornato al 2025.
Per la Ditta di manutenzione è stato predisposto il Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI), aggiornato al 2023.

Le Strutture aziendali incaricate della gestione della documentazione inerente alla materia, quali autorizzazioni/certificazioni/nullaosta rilasciati dalla Pubblica Amministrazione, sono tenute al rispetto dei principi di comportamento stabiliti e descritti nel protocollo "*Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione*".
La politica aziendale in tema di salute e sicurezza sul lavoro deve essere diffusa, compresa, applicata ed aggiornata a tutti i livelli organizzativi. Le linee d'azione generali della Sede Secondaria devono essere orientate verso un costante miglioramento della qualità della sicurezza e devono contribuire allo sviluppo effettivo di un "sistema di prevenzione e protezione". Tutte le Strutture della Sede Secondaria devono osservare le disposizioni in materia di salute, di sicurezza e di igiene del lavoro e tenerne conto in occasione di qualsivoglia modifica degli assetti esistenti, compresi ristrutturazioni/allestimenti di siti operativi.

10.4.2 Formazione

- La formazione obbligatoria dei dipendenti in materia di salute e sicurezza sul lavoro è erogata e tracciata, con aggiornamento periodico ogni cinque anni.
- Per i neoassunti, la formazione è svolta il giorno stesso dell'assunzione tramite piattaforma e-learning e fa parte del percorso di onboarding.
- La formazione dei lavoratori esterni (appaltatori) è a carico delle imprese appaltatrici, come previsto contrattualmente.

10.4.3 Gestione degli infortuni

Gli infortuni registrati negli ultimi anni sono stati sporadici e di lieve entità.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

10.4.4 Descrizione del processo

Il processo di gestione dei rischi in materia di salute e sicurezza sul lavoro prevede le seguenti fasi:

- identificazione dei pericoli e loro classificazione (pericoli per la sicurezza e pericoli per la salute dei lavoratori);
- valutazione dei rischi;
- individuazione e predisposizione delle misure di prevenzione e di protezione;
- definizione di un piano di intervento con l'identificazione delle strutture aziendali competenti all'attuazione di detti interventi;
- realizzazione, degli interventi pianificati nell'ambito di un programma;
- verifica dell'attuazione e controllo sull'efficacia delle misure adottate. Con specifico riferimento alla gestione dei cantieri (artt. 88 e seguenti del Testo Unico) che è nella responsabilità del "Committente", il processo prevede le seguenti fasi:
- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi;
- designazione del Responsabile dei lavori e, ove necessario del Direttore dei Lavori, del Coordinatore per la progettazione e del Coordinatore per l'esecuzione dei lavori, previa verifica dei requisiti professionali dei soggetti incaricati, e formalizzazione per iscritto dei relativi incarichi;
- pianificazione delle fasi di lavorazione e loro valutazione con particolare riferimento alle interazioni delle attività interferenti anche al contorno del cantiere ed alla eventuale compresenza di attività della Sede Secondaria e predisposizioni dei piani di sicurezza e coordinamento ovvero, ove non previsti dalla norma dei documenti di valutazione dei rischi interferenziali, anche per il tramite di professionisti incaricati;
- redazione delle lettere di richiesta di offerta con informativa alla controparte di quanto predisposto in tema di sicurezza (piani di sicurezza e coordinamento/documenti di valutazione dei rischi interferenziali);
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza, inerenti alle misure per gestire le interferenze, in relazione all'entità e alle caratteristiche del servizio/fornitura offerti nonché

contenente dichiarazione di presa visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- esecuzione degli adempimenti tecnico-amministrativi, notifiche e comunicazioni alla Pubblica Amministrazione, anche per il tramite dei professionisti incaricati;
- aggiudicazione del servizio e stipula del contratto, con l'indicazione dei costi per la sicurezza e allegazione del piano di sicurezza e coordinamento/documento di valutazione dei rischi interferenziali;
- coordinamento nell'esecuzione delle attività fra le imprese/lavoratori autonomi e controlli sul rispetto delle misure nel cantiere, anche per il tramite dei professionisti incaricati.

Nei cantieri temporanei o mobili allestiti in unità operative ove sono presenti collaboratori della Sede Secondaria i rischi derivanti da interferenze tra le due attività sono gestiti dal Committente, anche per il tramite di professionisti all'uopo incaricati, individuando le specifiche misure di prevenzione, protezione ed emergenza a tutela della salute e sicurezza dei collaboratori, dei clienti e delle imprese appaltatrici e lavoratori autonomi. Tali misure sono indicate nel Piano di Sicurezza e Coordinamento o, ove non previsto, nel Documento unico di valutazione dei rischi interferenziali (in relazione al rispettivo campo di applicazione) elaborato a cura dei soggetti individuati dal Committente, che può avvalersi anche del supporto della struttura di Prevenzione e Protezione del Datore di Lavoro della Sede Secondaria.

Con specifico riferimento alla gestione dei contratti di appalto, contratti d'opera, contratti di somministrazione (rientranti nell'ambito di applicazione dell'art. 26 del Testo Unico) il processo prevede le seguenti fasi:
- inoltro di una comunicazione preventiva ai dipendenti per informare circa le operazioni previste.
- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi, inclusa la certificazione dei materiali impiegati in caso di installazioni o modifiche ambientali
- è prevista, ove necessario, l'inibizione temporanea degli accessi alle aree interessate.
- informativa alla controparte circa i rischi specifici presenti nei luoghi in cui è chiamata ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla attività oggetto del contratto, nonché ove previsto dalla normativa, predisposizione del Documento di Valutazione dei Rischi Interferenziali (DUVRI), da inviare all'offerente ai fini della formulazione dell'offerta e parte integrante del contratto, contenente le misure idonee per eliminare o ridurre i rischi relativi alle interferenze delle attività connesse all'esecuzione del contratto e contestuale redazione della lettera di richiesta d'offerta ove prevista;
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza inerenti alle misure per gestire le interferenze in relazione all'entità e alle caratteristiche del servizio/fornitura offerti nonché contenente dichiarazione di presa di
- visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- aggiudicazione del servizio e stipula del contratto, con l'indicazione dei costi per la sicurezza e allegazione del DUVRI;

- esecuzione del servizio/fornitura da parte dell'aggiudicatario e cooperazione e coordinamento con le imprese/lavoratori autonomi per gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, anche mediante reciproca informazione al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva ed i rischi insiti nell'eventuale compresenza di personale, collaboratori e clienti della Sede Secondaria;
- controllo sul rispetto degli adempimenti contrattuali nell'esecuzione delle attività.
- le attività vengono svolte sempre in presenza di un referente aziendale incaricato, per presidiare l'intervento e prevenire rischi di interferenza con il personale interno.

Per gli adempimenti prescritti dal citato art. 26 il Datore di Lavoro ha conferito apposita delega al Responsabile della funzione Immobili di Intesa Sanpaolo per le attività di competenza di tale funzione, che può prevedere ulteriore delega a soggetti specificatamente individuati.
Le procedure di gestione e di controllo del processo si basano su una chiara e formalizzata assegnazione di compiti e responsabilità con riferimento alle Strutture coinvolte (ivi compresi gli outsourcer esterni) nelle verifiche di conformità alle disposizioni tempo per tempo vigenti in tema di salute e sicurezza nonché su un coerente sistema di deleghe che disciplina le funzioni ed i poteri derivanti dagli obblighi normativi previsti dal Testo Unico. Le modalità operative per la gestione del processo e l'individuazione delle strutture/figure che hanno le responsabilità delle diverse fasi sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Il processo di gestione degli infortuni prevede le seguenti fasi:

- Comunicazione, ove possibile, al referente aziendale da parte del dipendente coinvolto.

- Attivazione della procedura interna per la gestione del caso, con apertura della pratica sulla base del referto medico e della prognosi.

- Diffusione della procedura ai dipendenti tramite regolamento interno pubblicato sull'intranet e inviato via e-mail ai nuovi assunti.

10.4.5 Principi di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:
- Livelli autorizzativi definiti nell'ambito del processo:
  - il sistema di gestione aziendale prevede la definizione di specifiche responsabilità e procedure al fine di consentire la piena attuazione della politica di salute e sicurezza sul lavoro con un approccio sistematico e pianificato. In particolare, sono state individuate le figure aziendali che rivestono il ruolo rispettivamente di "Datore di Lavoro" e "Committente". Tali figure possono impartire disposizioni in materia alle Strutture aziendali e

godono della più ampia autonomia organizzativa e dispongono dei più ampi poteri di spesa, anche con facoltà di delega e subdelega ai sensi dell'art. 16 comma 3 bis del Testo Unico;
- è prevista un'articolazione di distinte funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
- tutti i soggetti/figure aziendali che intervengono nelle fasi del processo sopra descritto devono essere individuati e autorizzati con espressa previsione della normativa interna o tramite delega, da conferirsi e conservarsi a cura del Datore di Lavoro/Committente, ovvero a cura dei soggetti da costoro facoltizzati.

- La gestione della sicurezza è affidata a un referente aziendale designato (Office Manager) in coordinamento con il Dipartimento HR e con il supporto di un RSPP esterno.
- È garantita la presenza di un DVR aggiornato periodicamente, redatto in collaborazione con l'RSPP esterno, con aggiornamenti a fronte di variazioni organizzative, layout o piani di evacuazione.
- Segregazione dei compiti tra i differenti soggetti/figure aziendali coinvolte nel processo di gestione dei rischi in materia di salute e sicurezza sul lavoro. In particolare:
  - le strutture operative che hanno il compito di realizzare e di gestire gli interventi (di natura immobiliare, informatica, di sicurezza fisica, ovvero attinenti a processi di lavoro e alla gestione del personale), sono distinte e separate dalla Struttura alla quale, per legge e/o normativa interna, sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
  - le strutture competenti designano i soggetti ai quali sono attribuite specifiche mansioni per la gestione/prevenzione dei rischi per la sicurezza e la salute sul lavoro;
  - i Rappresentanti dei Lavoratori per la Sicurezza collaborano attivamente col Datore di Lavoro al fine di segnalare criticità ed individuare le conseguenti soluzioni.
  - In caso di attività di manutenzione o pulizia, è previsto un presidio operativo da parte del referente aziendale, con comunicazione preventiva ai dipendenti e gestione degli spazi per evitare interferenze.
- Attività di controllo:
  - le strutture competenti devono attivare un piano aziendale di controllo sistematico al fine di verificare periodicamente la corretta applicazione/gestione nonché efficacia delle procedure adottate e delle misure messe in atto per valutare, in ottemperanza alle prescrizioni di legge, i luoghi di lavoro. Il piano, in particolare, deve contemplare:
    - aree e attività aziendali da verificare (tra le quali le attività di natura organizzativa[40], di sorveglianza sanitaria, di informazione e formazione dei lavoratori, di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori);
    - modalità di esecuzione delle verifiche, modalità di rendicontazione;
    - Il piano aziendale deve altresì assicurare:
    - il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
    - l'acquisizione di documentazioni e certificazioni obbligatorie di legge

(relative ad edifici, impianti persone, società ecc.) da parte delle competenti strutture;
- il rispetto del processo e degli adempimenti tecnici ed amministrativi previsti dalle normative interne e di legge.

Deve inoltre prevedere un idoneo sistema di controllo sulla sua efficace attuazione e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del piano devono essere adottati quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

- le Strutture competenti devono controllare che tutte le misure di prevenzione e protezione programmate siano attuate, assicurando un costante monitoraggio delle situazioni di rischio e dell'avanzamento dei programmi di intervento previsti dagli specifici documenti di valutazione dei rischi. Tali Strutture si avvalgono, laddove occorra, della collaborazione della Struttura deputata alla gestione delle risorse umane, nonché delle strutture di gestione e realizzazione di interventi immobiliari, di progettazione e gestione dei processi lavorativi, della sicurezza fisica, dei sistemi informativi, di gestione e manutenzione;
- i Rappresentanti dei Lavoratori per la Sicurezza, nel rispetto delle norme di legge in materia, possono accedere alla documentazione aziendale inerente alla valutazione dei rischi e le misure di prevenzione relative e chiedere informazioni al riguardo. I medesimi Rappresentanti possono accedere ai luoghi di lavoro e formulare osservazioni in occasione di visite e verifiche da parte delle Autorità competenti;
- tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente ed il Responsabile del Servizio Prevenzione e Protezione visitano i luoghi di lavoro ove sono presenti lavoratori esposti a rischi specifici ed effettuano a campione sopralluoghi negli altri ambienti;
- figure specialistiche di alta professionalità e con i titoli ed i requisiti previsti dalle norme specifiche, preventivamente valutate, contribuiscono alla valutazione ed alla elaborazione di misure di tutela nel caso di rischi specifici (ad es. amianto, radon, elevato rischio di incendio) nonché nei cantieri temporanei e mobili (Responsabili dei lavori, Coordinatori per la Sicurezza, Progettisti, Direttori dei lavori ecc.);
- le competenti Strutture individuate dal Datore di Lavoro/Committente provvedono alla verifica dell'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare;
- le competenti strutture individuate dal Committente verificano l'idoneità tecnico-professionale dei Responsabili dei Lavori e dei Coordinatori per la progettazione e per l'esecuzione, avute presenti anche le specifiche caratteristiche dei lavori oggetto di contratti di appalto;
- qualora la documentazione prevista dal Testo Unico sia tenuta su supporto informatico, la competente Struttura verifica che le modalità di memorizzazioni dei dati e di accesso al sistema di gestione della predetta documentazione assicurino quanto previsto dall'art. 53 del Testo Unico;
- il Datore di Lavoro ed il Committente, ciascuno negli ambiti di competenza, vigilano ai sensi del comma 3 bis dell'art.

- 18 del Testo Unico in ordine all'adempimento degli obblighi in materia che la legge attribuisce a preposti, lavoratori, medici competenti, progettisti, fabbricanti, fornitori, installatori attraverso il piano aziendale di controllo sistematico sopra indicato;
- con riferimento ai cantieri temporanei o mobili, il Committente verifica il corretto conferimento degli incarichi e l'adempimento degli obblighi posti a carico del Direttore dei Lavori, del Responsabile dei Lavori, del Coordinatore per la progettazione e del Coordinatore per l'esecuzione dei lavori, ove nominati; a tal fine acquisisce dagli stessi apposite relazioni periodiche che diano conto dell'attività svolta, delle eventuali criticità emerse e delle misure adottate per la loro soluzione;
- È garantita la verifica periodica dell'idoneità tecnico-professionale degli appaltatori, con raccolta e aggiornamento della documentazione relativa alle imprese e ai lavoratori autonomi. La società segue la procedura KYP (Know Your Partner) prima dell'onboarding oppure al verificarsi di alcuni aggiornamenti rilevanti nella struttura della controparte
- Per tutte le attività in appalto è prevista la predisposizione dei DUVRI, aggiornati in caso di variazioni societarie o contrattuali.
- La gestione della sicurezza si svolge sotto la supervisione del referente aziendale designato (Office Manager) con il coordinamento della funzione People and Culture (funzione HR).

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - l'impiego di sistemi per la gestione informatica dei dati e della documentazione prescritta dal Testo Unico deve avvenire nel rispetto dell'art. 53 del medesimo;
  - ciascuna Struttura di volta in volta interessata, al fine di consentire la ricostruzione delle responsabilità, deve dotarsi di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività, ed è responsabile dell'archiviazione e della conservazione dei contratti stipulati nonché di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rischi in materia di sicurezza e salute dei lavoratori nonché della relativa attività di controllo;
  - ciascuna Struttura di volta in volta interessata è responsabile altresì dell'acquisizione della conservazione e dell'archiviazione di documentazioni e certificazioni obbligatorie di legge nonché della documentazione comprovante i requisiti tecnico-professionali delle imprese appaltatrici, dei lavoratori autonomi e dei soggetti destinatari di deleghe in materia di sicurezza (es.: Responsabile dei Lavori, Coordinatori per la progettazione e l'esecuzione);
  - la gestione dei diversi contesti di rischio prevede l'utilizzo di specifici sistemi informativi che consentano l'accesso in rete a tutte le Strutture interessate ed autorizzate alla valutazione dei rischi delle unità operative e che contengano, ad esempio, la documentazione tecnica di impianti, macchine, luoghi di lavoro ecc.., le liste degli esposti a specifici rischi, la documentazione sanitaria (con il rispetto dei requisiti di riservatezza previsti dalla normativa), le attività di formazione ed informazione, le attività di eliminazione/riduzione dei rischi, l'attività ispettiva interna ed esterna, le informazioni in tema di

infortuni e segnalazioni di rischio, la modulistica per la gestione dei monitoraggi ambientali e della **cartella sanitaria ecc.**

10.4.6 Gestione degli infortuni

La gestione degli infortuni segue una procedura interna codificata: i dipendenti devono segnalare tempestivamente l'evento al referente aziendale, che assiste nella gestione operativa e amministrativa della pratica.

10.4.7 Presidi operativi in materia di salute e sicurezza sul lavoro

- Gestione delle situazioni di emergenza;
- Svolgimento periodico di esercitazioni antincendio;
- Gestione del Primo Soccorso, svolgimento di corsi formativi, senza periodicità predefinita;
- Gestione della sorveglianza sanitaria, comprendente la pianificazione delle visite mediche e il monitoraggio degli esiti, al fine di tutelare la salute dei lavoratori;

10.4.8 Principi di comportamento

Le Strutture della Sede Secondaria, a qualsiasi titolo coinvolte nella gestione dei rischi in materia di salute e sicurezza sul lavoro, come pure tutti i dipendenti, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.
In particolare, tutte le Strutture/figure sono tenute - nei rispettivi ambiti - a:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela e valutando la scelta delle attrezzature di lavoro nonché la sistemazione dei luoghi di lavoro;
- partecipare ai corsi di formazione obbligatoria e aggiornare le proprie conoscenze in materia di sicurezza.
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- astenersi dall'affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità qualificata e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es. Ispettorato del Lavoro, A.S.L., Vigili del Fuoco, etc.) in occasione di accertamenti/procedimenti ispettivi;
- provvedere, nell'ambito dei contratti di appalto, d'opera o di fornitura, ad informare le controparti sui rischi specifici dell'ambiente in cui sono destinate

ad operare e ad elaborare ed applicare le misure atte a governare in sicurezza le eventuali interferenze fra le imprese compresi gli eventuali lavoratori autonomi; evidenziando nei contratti per i quali sia prescritto i costi per la sicurezza;

- Predisporre i DUVRI per tutte le attività affidate in appalto e aggiornarli in caso di variazioni societarie o contrattuali.
- Non accedere ai locali durante gli interventi di manutenzione o pulizia se non autorizzati
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- Tutti i destinatari del Modello devono partecipare ai corsi di formazione obbligatoria e mantenere aggiornate le proprie competenze in materia di sicurezza.
- curare il rispetto delle normative in tema di salute e sicurezza nei confronti di tutti i lavoratori non dipendenti, con particolare riferimento all'ambito nell'ambito dei contratti regolati dal D. Lgs n. 276/2003 e successive modifiche ed integrazioni, nonché nei confronti dei soggetti beneficiari di iniziative di tirocinio e dei terzi in genere che dovessero trovarsi nei luoghi di lavoro;
- assicurarsi che, nell'impiego di sistemi di elaborazione automatica dei dati, le modalità di memorizzazione dei dati e di accesso al sistema di gestione della documentazione prescritta garantiscano quanto previsto dall'art. 53 del Testo Unico.
- Garantire la riservatezza dei dati personali eventualmente trattati durante le attività lavorative, nel rispetto delle normative vigenti e delle policy interne.

Parimenti, tutti i dipendenti sono tenuti a:

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle Strutture aziendali e dalle Autorità competenti;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, ogni situazione di pericolo potenziale o reale, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tale situazione di pericolo.
- Seguire le procedure previste in caso di incidente o infortunio, informando immediatamente il referente aziendale preposto.
- Collaborare con il team preposto per garantire il rispetto dei protocolli di sicurezza.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti (anche omissivi) che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

10.5. Gestione del lavoro agile (*Smart Working*)

10.5.1 Premessa

La gestione del lavoro agile rappresenta un'attività sensibile ai fini del Modello 231, poiché implica l'adozione di strumenti e modalità operative che possono incidere sulla sicurezza delle informazioni, sulla tutela del patrimonio aziendale e sulla corretta gestione dei processi aziendali.
Younited S.A. – Sede Secondaria disciplina il lavoro agile attraverso una policy interna che regola gli aspetti organizzativi, tecnologici e di sicurezza correlati a tale modalità lavorativa.

10.5.2 Descrizione del processo

Il processo di gestione del lavoro agile si articola nelle seguenti attività:

- È prevista una policy interna dedicata allo smart working, che viene aggiornata annualmente e disciplina:
  - requisiti di ergonomia;
  - dotazione IT assegnata;
  - obblighi formativi per i dipendenti.
- Ogni anno viene sottoscritto da ciascun dipendente un accordo individuale di smart working, che è caricato nel portale "Quick Lavoro".
- Le giornate di lavoro da remoto sono tracciate tramite un applicativo HR, che registra la modalità di lavoro scelta dal dipendente.
- È in uso un sistema di badge, legati all'accesso fisico, non per il rilevamento dell'orario di lavoro) che viene consegnato ai dipendenti unitamente al regolamento per l'utilizzo dello stesso.
- La valutazione dei rischi specifici relativi al lavoro agile è stata inclusa nel Documento di Valutazione dei Rischi (DVR) 2023.

10.5.3 Principi di controllo

I presidi di controllo sul processo di gestione del lavoro agile sono i seguenti:

- Policy interna aggiornata annualmente, che definisce le regole per lo svolgimento del lavoro da remoto, le dotazioni tecnologiche e i requisiti ergonomici.
- Accordo individuale di smart working sottoscritto ogni anno, con archiviazione elettronica nel portale aziendale dedicato ("Quick Lavoro").
- Registrazione e tracciatura delle giornate in modalità agile tramite applicativo HR, per monitorare l'effettiva modalità di lavoro scelta.
- Sistema di badge utilizzato per motivi di sicurezza legati all'accesso fisico, non per il rilevamento dell'orario di lavoro.
- Valutazione dei rischi da lavoro agile inserita nel DVR 2023, a cura delle funzioni competenti.

10.5.4 Principi di comportamento

Tutti i dipendenti che aderiscono al lavoro agile devono:

- rispettare le disposizioni contenute nella policy interna e nell'accordo individuale di smart working;
- utilizzare le dotazioni IT aziendali in modo conforme alle regole di sicurezza informatica e alle policy di utilizzo dei dispositivi;

- garantire la tracciatura corretta delle giornate di lavoro da remoto tramite l'applicativo HR;
- partecipare alle attività formative obbligatorie previste dalla policy;
- rispettare le misure di sicurezza e le disposizioni in materia di tutela della salute e sicurezza previste dal DVR in relazione al lavoro agile.

10.6. Gestione dell'accesso di clienti e terzi agli spazi aziendali

10.6.1 Premessa

La gestione degli accessi di clienti, visitatori e consulenti agli spazi aziendali rappresenta un'attività sensibile per la tutela della sicurezza fisica, della riservatezza delle informazioni e della protezione dei dati personali trattati all'interno della Sede Secondaria.
Questa attività è regolata da procedure interne finalizzate a garantire il controllo degli ingressi, la tracciabilità degli accessi e la conformità alla normativa sulla protezione dei dati personali.

10.6.2 Descrizione del processo

Il processo di gestione degli accessi si articola come segue:

- L'accesso di visitatori e consulenti agli spazi aziendali è regolato da una comunicazione preventiva via e-mail da parte del referente interno.
- Gli ospiti sono sempre accompagnati dal referente interno durante la permanenza nei locali aziendali.

10.6.3 Principi di controllo

I principali controlli attivi e in fase di implementazione sono:

- Comunicazione preventiva via e-mail per autorizzare l'accesso di ospiti e consulenti.
- Accompagnamento obbligatorio degli ospiti da parte del referente interno, per garantire la sicurezza fisica e la protezione delle informazioni.

10.6.4 Principi di comportamento

Tutti i dipendenti e collaboratori coinvolti devono:

- attenersi alle procedure previste per la gestione degli accessi di terzi;
- garantire l'accompagnamento continuo degli ospiti all'interno dei locali aziendali;
- rispettare le misure di sicurezza interne, evitando comportamenti che possano compromettere la tutela del patrimonio aziendale o la riservatezza delle informazioni.

10.7. I flussi informativi all'Organismo di Vigilanza

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.
- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua verifiche ad evento, semestrali e annuali.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	**Descrizione del flusso informativo**	**Periodicità**
Office Manager	Segnalazione infortunio/near-miss con modulo e referto medico	Ad evento
Office Manager	Aggiornamento DUVRI/DVR o variazione layout/sicurezza	Ad evento
HR	Comunicazione apertura/chiusura pratica INAIL e report assenze	Ad evento
Office Manager	Report HSE semestrale: KPI infortuni, formazione completata, audit RSPP, stato DUVRI	Semestrale
RSPP	Attestazione di aggiornamento DVR e relazione sopralluoghi	Annuale

11 REATI DI CRIMINALITÀ INFORMATICA

11.1. Premessa

La presente Parte Speciale ha l'obiettivo di illustrare i criteri, i ruoli e le responsabilità, i principi di controllo e le regole di comportamento cui tutti i Destinatari del Modello, ivi compresi i consulenti, il personale, i fornitori e i

partner, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dagli articoli 24-*bis* del Decreto , nel rispetto dei principi di legalità, correttezza, oggettività, trasparenza, tracciabilità e riservatezza nell'esecuzione delle proprie attività, della normativa emanata dalle autorità di vigilanza e di tutte le leggi e le norme nazionali ed internazionali vigenti.

Quanto definito nella presente Parte Speciale si applica a tutte le unità organizzative coinvolte nei Processi a Rischio di seguito disciplinati nonché a tutte le funzioni di controllo deputate a vigilare sul rispetto e sull'adeguatezza delle procedure applicabili in materia di prevenzione dei reati in oggetto.

11.2. Le fattispecie di reati previste dagli artt. 24-*bis* del Decreto

La legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa, stipulata a Budapest il 23.11.2001, avente quale obiettivo la promozione della cooperazione internazionale tra gli Stati firmatari al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici, specie in considerazione della natura di tali illeciti, che spesso, nelle modalità della loro preparazione o realizzazione, coinvolgono Paesi diversi.
La riforma della disciplina della criminalità informatica è stata realizzata sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti. L'art. 7 della legge ha inoltre aggiunto al D. Lgs. n. 231/2001 l'art. 24 bis, che elenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli enti.
La citata legge ha modificato anche il codice di procedura penale e le disposizioni in tema di protezione dei dati personali, essenzialmente al fine di agevolare le indagini sui dati informatici e consentire per determinati periodi la conservazione dei dati relativi al traffico telematico.
Non sono invece state recepite nell'ordinamento italiano le definizioni di "sistema informatico" e di "dato informatico" contenute nella Convenzione di Budapest; tali definizioni, che si riportano qui di seguito, potranno essere prese come riferimento dalla giurisprudenza in materia:

- "sistema informatico": qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati;
- "dato informatico": qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

A titolo esaustivo, si precisa che il Decreto Legge 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*" ha introdotto all'interno dell'art. 24 *bis* i delitti in materia di *cybersecurity* di cui all'art. 1, comma 11, D.L. 21 settembre 2019,
n. 105.
Tuttavia, dato il perimetro di applicazione della norma (che si rivolge a enti e operatori, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale

dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale) i delitti introdotti all'interno dell'art. 24 bis non assumono rilevanza per Younited.

Si illustrano qui di seguito i reati presupposto elencati dall'art. 24 bis del D. Lgs. n. 231/2001.

Accesso abusivo ad un sistema telematico o informatico (Art. 615-TER C.P.) Il reato è commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo.
Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici.
Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell'interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema.
Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della Sede Secondaria (o anche di terzi concesse in licenza alla Sede Secondaria), mediante l'utilizzo delle credenziali di altri colleghi abilitati.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (Art. 615-quater c.p.) Tale reato si realizza quando un soggetto, "al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo".
Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici.

Per mezzo dell'art. 615-quater c.p., pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

Rientrano in questa categoria, ad esempio, codici di accesso, password, schede informatiche, badge, carte di credito, bancomat, smart card o altri strumenti

idonei a bypassare i sistemi di protezione informatica.

Un caso concreto può essere quello di un dipendente che, pur essendo autorizzato a operare con un certo livello di accesso al sistema informatico aziendale, acquisisce abusivamente credenziali o strumenti per ottenere un accesso di livello superiore, sfruttando la propria posizione o utilizzando tecniche fraudolente per appropriarsi di codici riservati.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.) e detenzione, diffusione e installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617- quinquies c.p.)
La condotta punita dall'art. 617-quater c.p. consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento o interruzione delle stesse. Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni.
L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. ad esempio *spyware*). L'impedimento od interruzione delle comunicazioni (c.d. "*Denial of service*") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime comunicazioni fittizie.
Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema.

L'art. 617-quinquies c.p., invece, punisce chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative a un sistema informatico o telematico o di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi idonei a tali scopi.
Nel contesto aziendale, tale reato potrebbe configurarsi, ad esempio, quando un dipendente o un collaboratore installa o mette a disposizione, senza autorizzazione, un software o un dispositivo che consenta di captare dati o bloccare le comunicazioni tra sistemi informatici, anche se non procede poi all'effettivo utilizzo di tali strumenti.

Estorsione mediante la commissione di reati informatici (art. 629 comma 3 c.p.) La Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della Cybersicurezza nazionale e di reati informatici" ha introdotto la nuova fattispecie di "estorsione mediante la commissione di reati informatici" all'art. 629, comma 3 c.p. che sanziona chi, al fine di conseguire un profitto ingiusto con altrui danno, costringe taluno a fare o a omettere qualcosa, mediante la realizzazione o la minaccia di realizzazione di uno o più reati

informatici o telematici.
La fattispecie si inserisce nella più ampia categoria dei reati estorsivi, ma si distingue per la specificità del mezzo utilizzato: le condotte informatiche o telematiche diventano strumento per coartare la volontà della vittima.
La pena prevista è della reclusione da sei a dodici anni e della multa. La pena è, invece, della reclusione da otto a ventidue anni se concorre taluna delle circostanze indicate all'art. 628, comma 3 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.
Un esempio pratico di questa fattispecie potrebbe verificarsi nel caso in cui un esponente aziendale comprometta o limiti deliberatamente l'operatività di un sistema informatico o di un dispositivo, subordinandone il ripristino al pagamento di una somma di denaro da parte del legittimo titolare

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) Tale fattispecie reato si realizza quando un soggetto "distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui". Tale reato è punito con la reclusione da due a sei anni.
La pena è della reclusione da tre a otto anni se il fatto è commesso:

i. da un pubblico ufficiale o da un incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri o da chi esercita, anche abusivamente, la professione di investigatore privato o con abuso della qualità di operatore del sistema;

ii. se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.

Il reato si configura, ad esempio, quando un soggetto cancella dati o informazioni memorizzate su un computer o su altro sistema informatico, senza aver ricevuto preventiva autorizzazione dal legittimo titolare del dispositivo.
Il danneggiamento può inoltre realizzarsi nell'interesse dell'ente quando, ad esempio, un soggetto alteri o elimini file o programmi informatici appena acquisiti, con lo scopo di eliminare le evidenze relative a un credito vantato da un fornitore, oppure per contestare falsamente l'esecuzione regolare delle prestazioni contrattuali da parte di quest'ultimo.

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.) L'art. 635 bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui.
Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.
L'art. 635 ter c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi

pertinenti, o comunque di pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.
Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio.
Qualora le condotte descritte conseguano ad un accesso abusivo al sistema esse saranno punite ai sensi del sopra illustrato art. 615 ter c.p.

Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)
Questo reato di realizza quando un soggetto "mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), 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".

La pena è aumentata se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con violenza alla persona o con minaccia ovvero se è armato.

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus).

Detenzione, diffusione e installazione abusivo di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.) L'art. 635-quater.1 c.p., introdotto dalla Legge 28 giugno 2024, n. 90 (cd. "Legge sulla Cybersicurezza"), ha sostituito l'abrogato art. 615-quinquies c.p., ridefinendo e ampliando la disciplina relativa alla diffusione e detenzione abusiva di strumenti informatici dannosi.
La norma punisce chi, al fine di danneggiare un sistema informatico o telematico, le relative informazioni, dati o programmi, ovvero per favorire l'interruzione o l'alterazione del funzionamento di tali sistemi, si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna, mette a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici idonei a causare tali danni o malfunzionamenti.

Un caso esemplificativo si verifica quando un dipendente, con l'obiettivo di favorire l'ente, diffonde o introduce all'interno del sistema informatico di un soggetto concorrente un software dannoso (quale un virus o un malware), capace di compromettere l'operatività del sistema, alterarne il funzionamento o provocarne l'interruzione, arrecando un danno all'avversario e generando un indebito vantaggio competitivo per l'organizzazione.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.) L' art. 635-quater c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis, 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. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.
L'art. 635-quinquies c.p. punisce le medesime condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra espressamente fra gli "eventi" aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità.
In questa previsione, a differenza di quanto previsto all'art. 635 ter, non vi è più alcun riferimento all'utilizzo da parte di enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità"; non sarebbe cioè, da un lato, sufficiente l'utilizzo da parte di enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.
Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema.
È da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento. Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615 ter c.p.

Falsità nei documenti informatici (art. 491-bis c.p.) L'art. 491-bis c.p. dispone che ai documenti informatici pubblici aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.
Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nell'attribuibilità allo stesso di un'efficacia probatoria secondo le norme civilistiche[41].
Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato (anche da parte dell'autore originario) successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate.
Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione.

Non sembrano poter trovare applicazione, con riferimento ai documenti informatici, le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487, 488 c.p.).
Il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.) Tale reato è commesso dal 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 danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato[42]. Il soggetto attivo del reato può essere evidentemente soltanto un soggetto "certificatore qualificato", che esercita particolari funzioni di certificazione per la firma elettronica qualificata.
A tale specifico proposito si osserva che la Sede Secondaria non riveste la qualifica di "certificatore qualificato" e che quindi tale disposizione non è di immediato interesse per la stessa. Si tenga comunque presente che – per assumere rilevanza penale – la violazione degli obblighi per il rilascio di un certificato qualificato deve essere assistita dal dolo specifico sopra evidenziato (perseguimento di un ingiusto profitto / danno altrui).

Ostacolo alle procedure in tema di definizione, gestione e controllo del "perimetro di sicurezza nazionale cibernetica" (art. 1, comma 11 d.l. n. 105/2019) Il reato punisce chi, allo scopo di ostacolare o condizionare le Autorità preposte a tutelare il sistema delle infrastrutture tecnologiche strategiche:

1. fornisce informazioni, dati o elementi di fatto non rispondenti al vero rilevanti:
   a. per la predisposizione e aggiornamento degli elenchi delle reti, dei sistemi (comprensivi della relativa architettura e componentistica) e dei servizi informatici della PA e degli operatori pubblici e privati con sede in Italia, dai quali dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di servizio essenziale per le attività civili, sociali o economiche fondamentali e dal cui malfunzionamento, interruzione o abuso possa derivare un pericolo per la sicurezza nazionale;
   b. ai fini delle comunicazioni che detti operatori pubblici e privati devono effettuare al CVCN (Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello Sviluppo economico) dei contratti di fornitura che intendano stipulare per approvvigionarsi di beni, sistemi e servizi ICT destinati a essere impiegati nelle reti, sistemi e servizi di cui al punto che precede;
   c. per lo svolgimento delle attività ispettive e di vigilanza concernenti il rispetto delle disposizioni e procedure inerenti alla predisposizione e aggiornamento dei predetti elenchi, alla comunicazione delle forniture e alla notifica degli incidenti e alle misure di sicurezza relative ai sopra menzionati, sistemi, reti e servizi;
2. omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

* * *

Più in generale può osservarsi che alcune fattispecie di reati informatici in concreto potrebbero non presentare il requisito della commissione nell'interesse o a vantaggio della Younited indispensabile affinché possa conseguire la responsabilità amministrativa della stessa.
Per altro verso si ricorda che qualora fossero integrati tutti gli elementi previsti dal D. Lgs. n. 231/2001 la responsabilità della Younited potrebbe sorgere, secondo la previsione contenuta nell'art. 8 del Decreto, anche quando l'autore del reato non sia identificabile (dovrebbe quantomeno essere provata la provenienza della condotta da un soggetto apicale o da un dipendente, anche se non identificato), evenienza tutt'altro che improbabile nel campo della criminalità informatica, in ragione della complessità dei mezzi impiegati e dell'evanescenza del cyberspazio, che rendono assai difficile anche l'individuazione del luogo ove il reato stesso possa ritenersi consumato.
Va infine ricordato che anche l'art. 640 ter c.p., che punisce il delitto di frode informatica perpetrata ai danni dello Stato o di altro ente pubblico, costituisce reato presupposto della responsabilità amministrativa degli enti.

11.3. Le Attività Aziendali Sensibili

Le attività della Sede Secondaria nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione. La Sede Secondaria ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alle disposizioni di Vigilanza e alla normativa europea e nazionale in materia di protezione dei dati personali per prevenire e controllare i rischi in tema di tecnologia dell'informazione (IT) e di Cybersecurity, a tutela del proprio patrimonio informativo, della clientela e dei terzi.

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i comportamenti illeciti come sopra descritti sono:

- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale.
- Gestione degli accessi fisici ai locali e videosorveglianza e gestione delle violazioni di sicurezza segnalate da terzi.

Si riportano di seguito i protocolli che dettano i principi di controllo ed i principi di comportamento applicabili a dette attività e che si completa con la normativa aziendale di dettaglio che regolamenta le attività medesime. Tali protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalle altre società del Gruppo e/o *outsourcer* esterni.

11.4. Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale

11.4.1 Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria

coinvolte nella gestione e nell'utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale.
In particolare, si applica a:

- tutte le Strutture della Sede Secondaria coinvolte nella gestione e l'utilizzo dei sistemi informativi che si interconnettono/utilizzano software della Pubblica Amministrazione ovvero delle Autorità di Vigilanza;
- tutte le Strutture deputate alla progettazione, alla realizzazione o gestione di strumenti informatici, tecnologici o di telecomunicazioni;
- tutte le Strutture che hanno la responsabilità di realizzare interventi di tipo organizzativo, normativo e tecnologico per garantire la protezione del Patrimonio Informativo aziendale nelle attività connesse con il proprio mandato e nelle relazioni con i terzi che accedono al Patrimonio Informativo del Gruppo;
- tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzano i sistemi informativi della Sede Secondaria e trattano i dati del Patrimonio Informativo aziendale.

Ai sensi del D. Lgs. n. 231/2001, i relativi processi potrebbero presentare occasioni per la commissione dei delitti informatici contemplati dall'art. 24 bis, nonché del reato di frode informatica ai danni dello Stato o di altro Ente pubblico previsto dall'art. 640 ter del codice penale e richiamato dall'art. 24 del Decreto. Inoltre, mediante l'accesso alle reti informatiche potrebbero essere integrate le condotte illecite aventi ad oggetto le opere dell'ingegno protette.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Sede Secondaria, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

11.4.2 Descrizione del Processo

L'utilizzo e la gestione di sistemi informatici e del Patrimonio Informativo sono attività imprescindibili per l'espletamento del business aziendale e contraddistinguono la maggior parte dei processi della Sede Secondaria. Tra i sistemi informativi utilizzati dalla Sede Secondaria vi sono utenze per l'accesso alle piattaforme per l'espletamento di adempimenti verso la Pubblica Amministrazione che prevedano il ricorso a specifici programmi forniti dagli stessi Enti, ovvero la connessione diretta con gli stessi, e l'istallazione di componenti software ove previsto e richiesto dalla competente Pubblica Amministrazione.

Si rendono quindi necessarie una efficace e stringente definizione di norme e misure di sicurezza organizzative, comportamentali e tecnologiche e la realizzazione di attività di controllo, peculiari del presidio a tutela di una gestione e di un utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale in coerenza con la normativa vigente.
Alla luce delle considerazioni che precedono, di seguito si declinano i processi sui quali si basa il presidio posto in essere sulla gestione e sull'utilizzo dei sistemi

informatici e del Patrimonio Informativo aziendale.

- Il processo di gestione della sicurezza informatica si articola nelle seguenti fasi:

10.4.6.1.1 analisi del rischio IT e definizione dei requisiti di sicurezza informatica;
10.4.6.1.2 gestione Accessi Risorse Informatiche e Servizi di Sicurezza ICT;
10.4.6.1.3 gestione normativa e architettura di sicurezza informatica;
10.4.6.1.4 monitoraggio eventi sicurezza informatica e gestione eventi critici di sicurezza informatica;
10.4.6.1.5 sicurezza delle terze parti (classificazione e monitoraggio dei fornitori della Sede Secondaria e della Capogruppo);
10.4.6.1.6 diffusione della cultura di sicurezza informatica;
10.4.6.1.7 progettazione e realizzazione soluzioni di sicurezza informatica.

- Il processo di prevenzione frodi si articola nelle seguenti fasi:

10.4.6.1.8 identificazione delle misure atte al rafforzamento della prevenzione;
10.4.6.1.9 monitoraggio dell'evoluzione delle frodi informatiche e fisiche anche per quanto riguarda eventuali aspetti di sicurezza fisica correlati;
10.4.6.1.10 presidio delle attività necessarie all'intercettazione e alla soluzione delle minacce verso gli asset aziendali;
10.4.6.1.11 gestione delle comunicazioni con le Forze dell'Ordine.

- Il processo di gestione della sicurezza fisica si articola nelle seguenti fasi:

10.4.6.1.12 gestione protezione di aree e locali ove si svolge l'attività.

- Processo di Certificazione della Firma Elettronica

Il processo relativo al servizio di certificazione della firma elettronica per i contratti rilasciati direttamente dalla Sede Secondaria si articola nelle seguenti fasi:

1. Apertura del contratto – Avvio della pratica contrattuale e predisposizione della documentazione necessaria.
2. Registrazione del titolare – Inserimento dei dati identificativi del soggetto che sottoscriverà il contratto, con verifica della completezza e correttezza delle informazioni.
3. Identificazione preventiva del legale rappresentante – Verifica dell'identità del legale rappresentante attraverso strumenti di riconoscimento idonei (ad es. documenti ufficiali, procedure KYC o analoghe).
4. Gestione del certificato di firma elettronica – Comprende tutte le operazioni successive alla registrazione: sospensione, riattivazione, revoca, rinnovo e sblocco PIN).

Tutte le attività sono tracciate e svolte in conformità alle normative vigenti in materia di identificazione digitale, protezione dei dati e firme elettroniche qualificate.
Il processo relativo alla progettazione, sviluppo e attivazione dei servizi ICT si articola nelle seguenti fasi:

- progettazione, realizzazione e gestione delle soluzioni applicative e delle infrastrutture tecnologiche aziendali e di Gruppo.
- Il processo di gestione e supporto ICT si articola nelle seguenti fasi:
- erogazione dei servizi ICT;

- monitoraggio del funzionamento dei servizi ICT e gestione delle anomalie;
- assistenza agli utenti attraverso attività di Help desk e *problem solving*.

Le modalità operative per la gestione dei processi descritti sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

11.4.3 Principi di controllo

Fatti salvi i requisiti di sicurezza propri del software della Pubblica Amministrazione o delle Autorità di Vigilanza utilizzato dalla Sede Secondaria, il sistema di controllo a presidio dei processi descritti si fonda sui seguenti principi cardine: livelli autorizzativi, segregazione dei compiti, attività di controllo e tracciabilità.

11.4.4 Livelli Autorizzativi

- I livelli autorizzativi sono definiti per ciascuna fase operativa dei processi aziendali.
- La gestione delle abilitazioni avviene mediante profili di accesso differenziati in funzione delle mansioni svolte.
- Le variazioni dei profili sono eseguite esclusivamente dalle strutture deputate alla sicurezza logica, su richiesta delle funzioni interessate; tali funzioni sono responsabili della coerenza tra le abilitazioni richieste e le mansioni effettive.
- Ogni utente dispone di un unico profilo abilitativo, definito secondo il principio del minimo privilegio; in caso di trasferimento o modifica dell'attività, viene attribuito il profilo corrispondente al nuovo ruolo.

11.4.5 Segregazione dei Compiti

- Sono assegnati ruoli e responsabilità distinti nella gestione della sicurezza delle informazioni, presidiando:
  - indirizzo e governo della sicurezza;
  - progettazione, implementazione ed esercizio delle contromisure;
  - controllo delle misure adottate a tutela del patrimonio informativo.
- Sono definite responsabilità chiare per:
  - gestione eventi di sicurezza anomali, emergenze e comunicazioni alle Autorità;
  - predisposizione, validazione, emanazione e aggiornamento delle norme di sicurezza da parte di funzioni aziendali distinte rispetto a quelle operative;
  - sviluppo e manutenzione di software/applicazioni e controllo degli accessi fisici/logici, affidati a strutture diverse dagli utenti.
- Il processo di sviluppo e manutenzione delle applicazioni interne o in outsourcing è gestito con iter autorizzativo controllato e verificabile.

11.4.6 Attività di Controllo

Le attività di gestione e utilizzo dei sistemi informativi della Sede Secondaria e del patrimonio informativo aziendale sono soggette a controllo costante, attraverso:

- misure per la protezione delle informazioni e dei dati personali (riservatezza, integrità e disponibilità);
- soluzioni tecnologiche, organizzative e infrastrutturali di continuità operativa anche in situazioni di emergenza;
- tracciabilità delle modifiche apportate alle procedure informatiche e degli utenti che le hanno effettuate;
- log delle attività di verifica e controllo sulle modifiche.

Younited ha adottato un sistema di misure tecniche, organizzative e procedurali per prevenire i reati informatici e proteggere dati e infrastrutture digitali, in linea con le prescrizioni dell'art. 24-bis del D.Lgs. 231/2001.

11.4.7 Misure di Sicurezza Informatica della Casa Madre

- Le misure di sicurezza informatica sono definite e aggiornate dalla Casa Madre.
- L'azienda applica procedure interne coerenti con tali linee guida per proteggere dati, integrità dei sistemi e rispetto delle normative vigenti.
- Casa Madre, con cadenza periodica effettuala la verifica e certificazione periodica delle utenze, attraverso un processo strutturato per:
    - confermare la legittimità degli utenti abilitati;
    - aggiornare o revocare i diritti di accesso ai software e alle funzionalità di sistema;
    - garantire segregazione dei ruoli e tracciabilità delle operazioni.

11.4.8 Infrastruttura IT e Gestione Centralizzata

- Server e database aziendali sono centralizzati presso la Casa Madre, secondo elevati standard di sicurezza.
- L'infrastruttura IT è gestita centralmente (Roma) e utilizza il cloud Microsoft con configurazioni sicure predefinite.
- L'accesso alle infrastrutture avviene tramite canali sicuri e tracciabili, con spazi segregati per team.
- Tutte le attività e gli accessi sono registrati tramite sistemi di logging per audit e verifiche.

11.4.9 Gestione delle Utenze e dei Dispositivi

Tutte le utenze hanno autenticazione a due fattori (2FA), credenziali univoche e personali.
Tutti i dispositivi aziendali utilizzano VPN per connessioni cifrate e sicure.
Le password sono soggette a rotazione automatica ogni 3/6 mesi; mancato aggiornamento → blocco utenza.

11.4.10 Monitoraggio Attivo degli Incidenti Informatici

La Casa Madre collabora con un provider esterno specializzato in cyber threat intelligence. È previsto un monitoraggio continuo dei sistemi aziendali e la generazione automatica di ticket in caso di eventi sospetti.
Gli incidenti informatici che coinvolgono partner esterni prevedono report e misure correttive.

11.4.11 Politiche Aziendali e Formazione Continua

È stata predisposta una procedura scritta per i dipendenti, pubblicata sulla intranet aziendale (piattaforma SharePoint). Ogni nuova policy viene notificata automaticamente ai dipendenti.

I dipendenti seguono periodicamente moduli di formazione sulla cybersicurezza, suddivisi in più sessioni didattiche.

11.4.12 Gestione della Posta Elettronica e delle Segnalazioni

Tutti i dipendenti sono istruiti a riconoscere e segnalare e-mail sospette, con possibilità di mettere in quarantena i messaggi sospetti tramite strumenti automatizzati.

Younited dispone inoltre di un sistema interno per la gestione di phishing, spam e minacce informatiche, con possibilità per gli utenti di segnalare e-mail sospette tramite Outlook; tali e-mail vengono poste in quarantena.

11.4.13 Controlli su Applicazioni, Sistemi e Reti

- Separazione degli ambienti di sviluppo, collaudo e produzione.
- Protezione della documentazione di sistema (configurazioni, personalizzazioni, procedure operative).
- Misure per installazione, gestione e emergenze delle applicazioni in produzione.
- Rimozione di sistemi/applicazioni obsoleti.
- Pianificazione e gestione dei backup di sistemi e dati.
- Controllo sull'utilizzo di strumenti, apparecchiature e supporti di memorizzazione, inclusa custodia, riutilizzo, distruzione e trasporto.

- Monitoraggio delle applicazioni e prevenzione di software dannoso (antivirus e procedure di aggiornamento).
- Regole per lo scambio di informazioni via e-mail/siti web.
- Sicurezza delle reti di telecomunicazione e degli apparati.
- Procedure per progettazione, sviluppo e cambiamento dei sistemi/reti.
- Conformità sull'uso di materiali coperti da diritti di proprietà intellettuale.

11.4.14 Sviluppo e Manutenzione delle Applicazioni

- Contromisure per proteggere le informazioni gestite dalle applicazioni (riservatezza, integrità, disponibilità).
- Controlli di sicurezza nel processo di sviluppo per garantire accesso solo a persone autorizzate tramite strumenti esterni all'applicazione (identificazione, autenticazione e autorizzazione).

11.4.15 Gestione degli Incidenti di Sicurezza

- Canali e modalità di comunicazione per segnalazione tempestiva di incidenti o situazioni sospette.
- Attivazione dell'escalation e apertura dello stato di crisi ove necessario.

11.4.16 Tracciabilità dei Processi

- Tutti gli eventi e le attività effettuate (accessi, rettifiche, variazioni profili, ecc.) sono registrati nei log files.
- Transiti in ingresso/uscita nelle zone riservate sono rilevati con sistemi di tracciatura.
- La tracciabilità è compatibile con le norme vigenti e consente di ricostruire responsabilità e motivazioni delle scelte effettuate.
- Ogni struttura è responsabile dell'archiviazione e conservazione della documentazione di competenza, anche in formato elettronico.

11.4.17 Principi di comportamento

Le Aree della Sede Secondaria, a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e del Patrimonio Informativo aziendale sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

Tutti i destinatari del Modello devono attenersi alle seguenti regole:

- Utilizzare le credenziali personali esclusivamente per finalità aziendali e non

condividerle con terzi.
- Accedere ai sistemi aziendali solo tramite le modalità previste (VPN e autenticazione a due fattori).
- Segnalare tempestivamente qualsiasi tentativo sospetto di phishing, spam o accesso non autorizzato.
- Rispettare le policy aziendali in materia di sicurezza informatica pubblicate su SharePoint.
- Partecipare ai corsi obbligatori di formazione in materia di cybersecurity, completando i moduli nei tempi previsti.
- Collaborare attivamente con il team IT e con il SOC in caso di anomalie o eventi di sicurezza.
- Non alterare o disattivare i sistemi di sicurezza aziendali.

In particolare:
- le Strutture coinvolte nei processi devono predisporre e mantenere il censimento degli applicativi che si interconnettono con la Pubblica Amministrazione o con le Autorità di Vigilanza e/o dei loro specifici software in uso;
- i soggetti coinvolti nel processo devono essere appositamente incaricati;
- ogni dipendente/amministratore del sistema è tenuto alla segnalazione all'Alta Direzione aziendale di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente ed attivando l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi ed alle comunicazioni alle Autorità Preposte;
- ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Sede Secondaria dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi informatici e del Patrimonio Informativo aziendale nonché nell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001 e, più in particolare, a titolo meramente esemplificativo e non esaustivo:

- introdursi abusivamente direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Sede Secondaria e del Gruppo, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, troian, spyware, dialer, keylogger, rootkit, ecc…) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre, o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:
  - diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;
  - abusivamente duplicare, detenere o diffondere in qualsiasi forma programmi per elaboratore od opere audiovisive o letterarie;
  - detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di

protezione dei programmi di elaborazione;
- riprodurre banche di dati su supporti non contrassegnati dalla SIAE, diffonderle in qualsiasi forma senza l'autorizzazione del titolare del diritto d'autore o in violazione del divieto imposto dal costitutore;
- rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;
- importare, promuovere, installare, porre in vendita, modificare o utilizzare, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

11.5. Gestione degli accessi fisici ai locali e videosorveglianza e gestione delle violazioni di sicurezza segnalate da terzi

11.5.1 Premessa

La Sede Secondaria tutela l'integrità e la sicurezza fisica delle proprie infrastrutture attraverso controlli sugli accessi ai locali e sistemi di videosorveglianza, al fine di prevenire intrusioni, sottrazioni di asset informativi e danni ai sistemi.

Tali attività rientrano tra quelle sensibili ai fini del D.Lgs. 231/2001, in quanto potrebbero rappresentare occasioni per la commissione di reati informatici, appropriazione indebita, danneggiamento o altre condotte illecite rilevanti per la responsabilità amministrativa degli enti.

11.5.2 Descrizione del processo

La gestione della sicurezza fisica e delle violazioni segnalate si articola nelle seguenti attività operative:
- Controllo accessi ai locali:
  - Introduzione di badge personali per il personale dipendente.
- Sistemi di allarme e videosorveglianza:
  - Impianto di allarme collegato a servizio di vigilanza esterna
  - Videosorveglianza attiva sugli ingressi, con cartellonistica informativa conforme alle disposizioni di legge.
- Gestione delle violazioni di sicurezza segnalate da terzi:
  - In caso di violazione segnalata da fornitore, è prevista la richiesta formale di un report entro 48 ore, contenente:
    - descrizione dell'evento;
    - dati eventualmente compromessi;
    - contromisure adottate.

11.5.3 Principi di controllo

Il sistema di controllo si fonda sui seguenti principi:

- Identificazione e tracciabilità degli accessi:
  - Tutti gli accessi fisici dei dipendenti sono registrati e tracciati tramite badge personali.
  - Sono conservati i log degli accessi per un periodo definito dalla normativa interna.
- Monitoraggio mediante videosorveglianza:
  - La videosorveglianza è attiva solo negli orari e nei perimetri autorizzati, con registrazione conforme alle norme privacy e comunicazione agli organi competenti.
- Gestione tempestiva delle segnalazioni di sicurezza:
  - In caso di alert o segnalazione di incidenti da parte di terzi, è previsto un processo formale di richiesta e analisi del report entro 48 ore, al fine di valutare l'impatto per la Sede Secondaria.
- Coinvolgimento dell'Organismo di Vigilanza e delle funzioni di controllo in caso di violazioni potenzialmente rilevanti ai fini del D.Lgs. 231/2001.

11.5.4 Principi di comportamento

Tutti i dipendenti, che accedono ai locali della Sede Secondaria, sono tenuti a:

- utilizzare correttamente i badge di accesso, evitando cessioni o usi impropri;
- segnalare tempestivamente all'unità competente ogni anomalia o tentativo di accesso non autorizzato;
- rispettare le disposizioni interne in materia di sicurezza fisica e videosorveglianza, comprese quelle derivanti dalla normativa sulla privacy;
- collaborare con i referenti della sicurezza nella gestione delle eventuali segnalazioni di violazioni provenienti da partner terzi.

È fatto divieto di porre in essere o collaborare a comportamenti che possano compromettere la sicurezza fisica e logica dei sistemi aziendali o che possano integrare una violazione delle norme in materia di protezione degli asset aziendali e informatici.

11.6. I flussi informativi all'Organismo di Vigilanza

Il sistema dei flussi informativi verso l'Organismo di Vigilanza è finalizzato a garantire un efficace presidio sul rispetto del Modello 231 e sull'emersione tempestiva di eventuali criticità. L'OdV ha il compito specifico di monitorare e verificare l'insorgenza di eventuali tematiche critiche o anomalie legate all'operatività aziendale.
I flussi informativi si articolano come segue:

- **Comunicazioni ad hoc su eventi**: le strutture aziendali e i soggetti coinvolti nelle aree a rischio sono tenuti a comunicare all'OdV, senza ritardo, ogni informazione relativa a eventi, situazioni o fatti che potrebbero rappresentare un rischio ai sensi del D.Lgs. 231/2001 o avere rilevanza ai fini della vigilanza.
- **Pianificazione degli interventi da parte dell'OdV**: a seguito delle

comunicazioni ricevute, l'OdV valuta la rilevanza delle informazioni, pianifica eventuali approfondimenti o interventi di verifica specifici e ne cura l'esecuzione, coordinandosi con le strutture aziendali competenti.

- **Verifiche periodiche**: oltre alle comunicazioni e verifiche puntuali, l'OdV effettua verifiche semestrali, annuali e ad evento.

Le modalità e i contenuti dei flussi informativi sono di seguito dettagliate:

Unità Organizzativa	**Descrizione del flusso informativo**	**Periodicità**
IT Security	Notifica **incidente critico:** data-breach interno, ticket SOC, blocco account per phishing.	Ad evento
IT Security	Comunicazione data-breach di partner con report dettagliato	Ad evento
IT Security	**Report Cyber semestrale**: account bloccati, KPI training, scadenze password.	Semestrale
IT e HR	**Formazione Cyber** (moduli e-learning)	Semestrale
IT	**Attestazione annuale** compliance policy IT, stato adeguamento NIS2, audit interni.	Annuale
Office Manager	Segnalazione **violazione accessi fisici**	Ad evento