

**MODELLO DI ORGANIZZAZIONE, GESTIONE E
CONTROLLO**

EX DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

**YOUNITED S.A., SEDE SECONDARIA
ITALIANA**



INDICE

DEFINIZIONI	5
PREMESSA	8
STRUTTURA DEL MODELLO	9
1. IL DECRETO LEGISLATIVO N. 231/2001	10
1.1. Caratteristiche fondamentali ed ambito di applicazione.	10
1.2. Il modello organizzativo come forma di esonero dalla responsabilità	12
1.3. L'apparato sanzionatorio.....	14
2. L'APPROCCIO METODOLOGICO ADOTTATO	16
2.1 La scelta della Sede Secondaria italiana	16
2.2 I Presupposti	17
2.3 Gli strumenti di governance adottati	18
2.5 Il processo di redazione e implementazione del Modello	21
2.5.1 Risk Assessment	22
2.5.2 Risultanze delle attività di <i>Risk Assessment</i>	24
2.5.3 Stesura del Modello di Organizzazione, Gestione e Controllo.....	25
3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO	26
3.1. Finalità e struttura del Modello	26
3.2. Natura del Modello e rapporti con il Codice Etico	27
3.3. Destinatari del Modello	28
3.4. Adozione, modifiche e integrazioni del Modello	29
4. ORGANISMO DI VIGILANZA	30
4.1. Identificazione dell'OdV	30
4.2. Modalità di nomina e revoca	30
4.3. Cause di ineleggibilità e motivi di revoca	31
4.4. Durata in carica dell'OdV	34
4.5. Funzioni dell'OdV	34
4.6. Obblighi di informazione verso l'Organismo di Vigilanza	37
4.7. Reporting dell'OdV	41
4.8. Conservazione delle informazioni.....	42
5. DIFFUSIONE DEL MODELLO	42
5.1. Comunicazione iniziale	42
5.2. Formazione del personale	43
6. SISTEMA DISCIPLINARE	45
6.1. Violazioni del Modello	45
6.2. Misure nei confronti dei dipendenti.....	46
6.3. Violazioni del Modello da parte dei dirigenti e relative misure	48
6.4. Misure nei confronti dei lavoratori in regime di distacco da altre società del Gruppo	50
6.5. Misure nei confronti dei Consulenti, collaboratori, Appaltatori	50
6.6. Misure nei confronti dell'Organo Dirigente	50
PARTE SPECIALE	52

1.	CARATTERISTICHE, STRUTTURA E OBIETTIVI DELLA PARTE SPECIALE	52
2.	LE COMPONENTI DEL SISTEMA DI CONTROLLO PREVENTIVO	53
2.1.	Sistema organizzativo.....	54
2.2.	Sistema autorizzativo.....	54
2.3.	Processo decisionale.....	54
2.4.	Controllo di gestione e flussi finanziari	55
2.5.	Programma di informazione e formazione	55
2.6.	Sistemi informativi e applicativi informatici.....	56
2.7.	Archiviazione della documentazione	56
3.	REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E IL SUO PATRIMONIO, REATI DI INTRALCIO ALLA GIUSTIZIA.....	57
3.1.	Premessa	57
3.2.	Fattispecie di reato previste dagli artt. 24, 25 e 25- <i>decies</i> e 25- <i>duodecies</i> del Decreto	58
3.3.	Le Attività Aziendali sensibili	63
3.3.1	Gestione dei rapporti contrattuali con la Pubblica Amministrazione.....	64
3.3.2	Gestione delle attività inerenti alla richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione	68
3.3.3	Gestione della formazione finanziata	72
3.3.4	Gestione dei contenziosi e degli accordi transattivi	77
3.3.5	Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali	82
3.3.6	Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni	86
3.3.7	Gestione del processo di selezione e assunzione del personale	91
3.3.8	Gestione dei rapporti con i Regolatori	95
4.	I REATI SOCIETARI	99
4.1.	Premessa	99
4.2.	Le fattispecie di reato previste dall'art 25- <i>ter</i> del Decreto.....	99
4.3.	Attività aziendali sensibili	101
4.3.1	Gestione dell'informativa periodica	101
5.	REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO, REATI DI CRIMINALITÀ ORGANIZZATA, REATI TRANSNAZIONALI	106
5.1.	Premessa	106
5.2.	Le fattispecie di reato previste dall'art. 25- <i>quater</i> del Decreto	106
5.3.	Attività aziendali sensibili	112
6.	REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI ED UTILITÀ DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO - REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO – DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI.....	113
6.1	Premessa	113

6.2	Le fattispecie di reato di cui agli artt. 25- <i>octies</i> , 25- <i>octies</i> .1. e 25- <i>quater</i> del Decreto.....	114
6.3	Attività Aziendali sensibili.....	121
6.3.1	Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose.....	122
7.	REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO	129
7.1	Premessa	129
7.2	Le fattispecie di reato previste dall'art. 25- <i>septies</i> del Decreto....	129
7.3	Le Attività Aziendali sensibili	130
7.3.1	Gestione dei rischi in materia di salute e sicurezza sul lavoro anche con riferimento all'attività svolta da appaltatori e subappaltatori	131
8.	REATI DI CRIMINALITÀ INFORMATICA.....	139
8.1.	Premessa.....	140
8.2.	Le fattispecie di reati previste dagli artt. 24- <i>bis</i> e 25- <i>novies</i> del Decreto.....	140
8.3.	Le Attività Aziendali Sensibili.....	146
8.3.1.	Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale.....	147
9.	REATI CONTRO L'INDUSTRIA ED IL COMMERCIO ED I REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE	156
9.1	Premessa	156
9.2	Le fattispecie di reato previste dall'articolo 25- <i>bis</i> e 25- <i>bis</i> 1 del Decreto e dell'art. 10 della l. 146/2006	156
9.3	Le Attività Aziendali sensibili	162
10.	REATI TRIBUTARI	162
10.1	Premessa	162
10.2	Le fattispecie di reato di cui all'art. 25- <i>quinqüesdecies</i> del Decreto	163
10.3	Le Attività Aziendali sensibili.....	164
10.3.1	Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari.....	165

DEFINIZIONI

“Appaltatori”	Convenzionalmente si intendono tutti gli appaltatori di opere o di servizi ai sensi del codice civile, nonché i subappaltatori, i lavoratori somministrati, i lavoratori autonomi che abbiano stipulato un contratto d’opera con la Sede Secondaria e di cui queste si avvalgono nei Processi a Rischio (cfr. <i>infra</i>)
“CCNL”	Contratto Collettivo Nazionale del Lavoro per il settore del commercio per i dipendenti da aziende del terziario, della distribuzione e dei servizi – Confcommercio.
“Consulenti”	Soggetti che agiscono in nome e/o per conto della Sede Secondaria sulla base di un mandato o di un altro rapporto di collaborazione
“CEO Italy”	Manager al quale compete il coordinamento e la rappresentanza della Succursale italiana (“Country Manager”).
“Codice Etico”	Documento redatto da Younited S.A. per il Gruppo
“DCM”	Debt Capital Markets
“Decreto”	Il Decreto Legislativo n. 231 dell’8 giugno 2001 e successive modificazioni
“Delega”	L’atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative
“Destinatari”	Tutti i soggetti cui è rivolto il Modello così come definiti nel paragrafo 3.3
“Ente”	La Sede Secondaria italiana Younited a norma del D.Lgs. 231/01

“Gruppo”	Il gruppo Younited, composto dalla capogruppo, Younited S.A., e dalle sedi estere dalla stessa direttamente controllate
“Modello”	Il Modello di organizzazione, gestione e controllo previsto dal Decreto e adottato dalla Sede Secondaria
“Organismo di Vigilanza o “OdV”	L’organismo di vigilanza della Sede Secondaria istituito ai sensi del Decreto
“Organo Dirigente”	Coloro che hanno ricevuto apposita delega dal consiglio di amministrazione di Younited S.A. per impegnare legalmente nei confronti dei terzi la Sede Secondaria
“Organo Dirigente” o “Organi Dirigenti”	Collettivamente indica gli Institori della Sede Secondaria
“Partner”	Controparti contrattuali della Sede Secondaria, con cui queste ultime avvengono ad una qualunque forma di collaborazione
“Processo a Rischio”	L’insieme di attività ed operazioni aziendali della Sede Secondaria organizzate al fine di perseguire un determinato scopo o gestire un determinato ambito aziendale, in aree potenzialmente a rischio di commissione di uno o più Reati, così come elencate nella Parte Speciale del Modello, indicate anche genericamente e complessivamente come area/e a rischio
“Procura”	Il negozio giuridico unilaterale con cui la Sede Secondaria attribuisce dei poteri di rappresentanza nei confronti dei terzi

“Reati”	Le fattispecie di reato e illecito amministrativo considerate dal Decreto
“Sede Secondaria “Younited o Succursale”	o Filiale italiana Younited S.A., registrata presso Banca d’Italia con autorizzazione n.8054 e codice ABI 3638
“Strutture”	Le varie Funzioni e Dipartimenti all’interno della Sede Secondaria italiana
“Testo Unico Bancario” o “TUB”	Il d.lgs. 1 settembre 1993, n. 385
“Testo unico della Finanza” o “TUF”	Il d.lgs. 24 febbraio 1998, n. 58
“Younited S.A.” o “la Società”, o la “Banca” o “la Casa Madre”, o “la Capogruppo”	Società costituita in Francia

PREMESSA

La Younited S.A. è una società fintech attiva nell'ambito del credito al consumo dal 2011 e presente nei principali mercati dell'Europa Continentale: Francia, Italia, Spagna, Portogallo e Germania.

Younited S.A. è portatrice di un innovativo modello che consente di coniugare l'esigenza dei privati di finanziare i propri consumi con l'interesse degli investitori a individuare nuove e diversificate fonti di rendimento per il loro portafoglio.

La Younited S.A. è una società costituita in base a leggi di altro stato (i.e. Francia) ed ha per oggetto *“la prestazione di consulenza finanziaria sia in Francia che all'estero; e, più in generale, qualsiasi operazione di qualsiasi natura, giuridica, economica e finanziaria, civile e commerciale.”*

Leader nel credito al consumo online in Francia, Younited S.A., a seguito dell'apertura di una propria Sede Secondaria in via Sardegna n. 40, 00187 Roma, è **presente sul mercato italiano dal 2016** dove si pone come la **prima fintech specializzata nel credito online che offre ai propri clienti le stesse garanzie di solidità e di trasparenza del circuito bancario tradizionale.**

STRUTTURA DEL MODELLO

Il presente Modello si struttura in una Parte Generale e in diverse Parti Speciali.

Nella **Parte Generale** sono riportati brevemente i contenuti del Decreto, le funzioni e i poteri attribuiti all'Organismo di Vigilanza, nonché i relativi flussi informativi, ed è contenuta una descrizione della struttura del Modello adottato dalla Sede Secondaria e del Sistema Disciplinare in essere.

Nelle **Parti Speciali** sono descritti i protocolli ovvero l'insieme di regole e di principi di controllo e di comportamento ritenuti idonei a governare i Processi a Rischio ovvero le aree di attività per le quali è stato rilevato un rischio di potenziale commissione dei Reati.

Gli Allegati, di volta in volta richiamati nel testo del documento, sono considerati parte integrante del Modello, ed in particolare sono così articolati:

- Allegato A: Codice Etico.

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 AG¹, 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 25²);
- 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-*quater*.1);
- i) **delitti contro la personalità individuale** (art. 25-*quinquies*);
- j) **reati e illeciti amministrativi di abuso di mercato** (art. 25-*sexies*);

¹ Caso in relazione al quale venne contestata la responsabilità per l'illecito di cui all'art. 25, c. 3 del D. Lgs. 231/2001 in capo alla società Siemens AG, avente sede in Germania, in relazione a fattispecie di corruzione poste in essere da dipendenti della medesima nei confronti di pubblici funzionari italiani, al fine di favorire la società nell'aggiudicazione di una serie di forniture di turbine a gas per il programma di riconversione delle centrali di Enel Produzione. Il 27 aprile 2004, il Tribunale di Milano, in funzione di G.i.p., applicò a Siemens AG la sanzione interdittiva del divieto di contrattare con la Pubblica Amministrazione italiana per la durata di un anno.

² Si segnala, altresì, che la Legge n. 69 del 27 maggio 2015 ha apportato modifiche alla disciplina sanzionatoria di alcuni dei reati presupposto considerati dall'art. 25, senza, tuttavia, intaccare il disposto di quest'ultimo.

- k) **reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies);**
- 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 o, come nel caso della sopra menzionata Legge 146/2006, l'emanazione di testi legislativi che, pur non modificando direttamente il Decreto, ne dispongano l'applicabilità – integrale o meno – ad ulteriori fattispecie di reato o illecito amministrativo.

1.2. Il modello organizzativo come forma di esonero dalla responsabilità

Il Decreto prevede che l'ente non risponda dei Reati commessi dai soggetti c.d. apicali qualora dimostri:

- di aver adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire Reati della specie di quelli verificatisi;
- di aver affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento;
- che le persone hanno commesso il reato eludendo fraudolentemente i suddetti modelli di organizzazione e di gestione;
- che non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per i Reati commessi da soggetti non in posizione apicale l'ente è responsabile solo qualora la commissione del Reato stesso sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. In ogni caso è esclusa l'omissione degli obblighi di direzione e vigilanza se, prima della commissione del Reato, l'ente ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto prevede inoltre che i suddetti Modelli debbano rispondere alle seguenti esigenze:

- a. individuare le attività che rendano possibile la commissione dei Reati;
- b. prevedere specifici protocolli (i.e. procedure) 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 ad impedire la commissione dei Reati;
- d. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli;
- e. introdurre un sistema disciplinare privato idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto prevede che gli enti, per soddisfare le predette esigenze, possano adottare modelli di organizzazione e di gestione "sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro trenta giorni osservazioni sulla idoneità dei modelli a prevenire i reati".

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 ricordare che le indicazioni ivi contenute rappresentano un semplice quadro di riferimento cui rifarsi ai fini dell'adozione di un modello. Si tratta di suggerimenti cui liberamente ispirarsi nell'elaborazione del Modello. Occorrerà, infatti, adeguare le Linee Guida alla propria concreta realtà e, quindi, alle dimensioni ed alla specifica attività svolta, scegliendo di conseguenza le modalità tecniche con cui procedere all'adozione del Modello.

E' opportuno evidenziare che un modello, oltre ad avere quale riferimento le indicazioni presenti nelle Linee Guida, deve essere personalizzato al fine di tenere conto delle peculiarità della società che lo adotta.

Inoltre, con specifico riferimento alla materia della salute e sicurezza sul luogo di lavoro, è doveroso ricordare che l'art. 30 del D. Lgs. 9 Aprile 2008, n. 81, stabilisce che, al fine di avere efficacia esimente della responsabilità amministrativa degli enti di cui al Decreto, il modello di organizzazione e

gestione deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- al rispetto degli standard legali, tecnici e strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Il suddetto modello organizzativo e gestionale deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività in precedenza elencate.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione dello stesso e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

Il riesame e l'eventuale modifica del modello organizzativo devono essere realizzati quando:

- siano scoperte violazioni significative delle norme relative alla tutela della salute e sicurezza sul lavoro, ovvero
- in occasione di mutamenti nell'organizzazione e nell'attività in conseguenza di progressi scientifici e tecnologici.

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'autorizzazione³).

³ Si veda a tale proposito l'art. 97-*bis* del Testo Unico Bancario e art 187-*quinquies* del Testo Unico della Finanza.

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 verificano 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 scritte⁴.

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 queste ultime e le aspettative dei loro 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.

⁴ Art. 97-bis del Testo Unico Bancario, così come inserito dall'art. 8 del D.L.vo 9 luglio 2004, n. 197 (Responsabilità per illecito amministrativo dipendente da reato) 1. "Il pubblico ministero che iscrive, ai sensi dell'articolo 55 del decreto legislativo 8 giugno 2001, n. 231, nel registro delle notizie di reato un illecito amministrativo a carico di una banca ne dà comunicazione alla Banca d'Italia e, con riguardo ai servizi di investimento, anche alla CONSOB. Nel corso del procedimento, ove il pubblico ministero ne faccia richiesta, vengono sentite la Banca d'Italia e, per i profili di competenza, anche la CONSOB, le quali hanno, in ogni caso, facoltà di presentare relazioni scritte. 2. In ogni grado del giudizio di merito, prima della sentenza, il giudice dispone, anche d'ufficio, l'acquisizione dalla Banca d'Italia e dalla CONSOB, per i profili di specifica competenza, di aggiornate informazioni sulla situazione della banca, con particolare riguardo alla struttura organizzativa e di controllo. 3. La sentenza irrevocabile che irroga nei confronti di una banca le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a) e b), del decreto legislativo 8 giugno 2001, n. 231, decorsi i termini per la conversione delle sanzioni medesime, e' trasmessa per l'esecuzione dall'Autorità giudiziaria alla Banca d'Italia. A tale fine la Banca d'Italia può proporre o adottare gli atti previsti dal titolo IV, avendo presenti le caratteristiche della sanzione irrogata e le preminenti finalità di salvaguardia della stabilità e di tutela dei diritti dei depositanti e della clientela. 4. Le sanzioni interdittive indicate nell'articolo 9, comma 2, lettere a) e b), del decreto legislativo 8 giugno 2001, n. 231, non possono essere applicate in via cautelare alle banche. Alle medesime non si applica, altresì, l'articolo 15 del decreto legislativo 8 giugno 2001, n. 231. 5. Il presente articolo si applica, in quanto compatibile, alle succursali italiane di banche comunitarie o extracomunitarie".

2.2 I Presupposti

La Sede Secondaria, 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 e riportate nella documentazione relativa al Risk Assessment⁵ a supporto 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.

Inoltre, al fine di garantire una rappresentazione sintetica ma al tempo stesso organica di tali strumenti organizzativi e di controllo, l'elenco aggiornato, delle policy, delle procedure e delle disposizioni organizzative rilevanti anche ai fini del Decreto è riportato nella documentazione relativa al Risk Assessment⁶ a supporto del Modello.

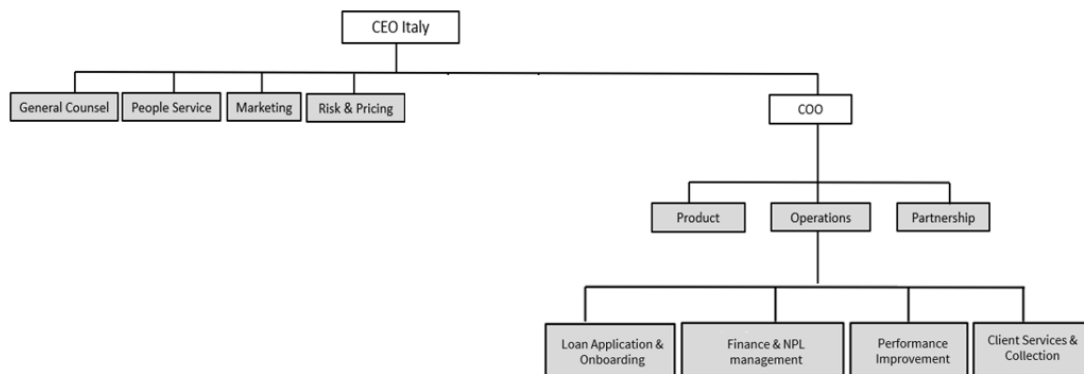
⁵ Si rimanda in particolare ai documenti riepilogativi dell'analisi dei rischi e dei controlli effettuata sulla base del confronto/condivisione con i responsabili di riferimento (Risk Assessment) e contenenti il riepilogo delle principali normative aziendali in essere per la gestione dell'attività.

⁶ Cfr. nota n. 5.

2.3 Gli strumenti di governance adottati

Ad oggi la Sede Secondaria italiana conta 72 dipendenti, numero destinato ad aumentare in relazione alla crescita del volume d'affari previsto.

L'organigramma della Succursale, aggiornato al 31 gennaio 2024, è così rappresentato:



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

Le decisioni strategiche finali restano in ogni caso sottoposte alla validazione del CEO di Gruppo e del 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, a seguito di una riorganizzazione effettuata a Settembre 2022, 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 stato delegato 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:

Il **Consiglio di Sorveglianza** 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 selezionati sono invitati a partecipare ad alcune commissioni quando necessario.

Il **Consiglio di Gestione** si avvale di comitati dedicati in funzione delle rispettive competenze, quale, a titolo esemplificativo, l'ALM (*asset liability management*), la performance dei fondi e il controllo interno con persone di management selezionate, tra cui, se necessario, il manager italiano del Paese. Il Consiglio di Gestione si avvale anche di un Comitato Esecutivo composto dai vertici delle linee di business Francia e dai CEO delle filiali.

2.4 Le caratteristiche salienti del sistema dei controlli interni

Il sistema dei controlli interni della Sede Secondaria è impostato dalla Casa Madre, che, in ottemperanza alla normativa europea, prevede un piano di controllo interno che include le attività di:

- supporto alla Sede Secondaria nel delineare le procedure chiave (le procedure locali sono basate sulle procedure europee già esistenti, recependo ogni specificità del paese della Sede Secondaria, in ottemperanza alla Direttiva 2008/48/CE del Parlamento Europeo e del Consiglio del 23 aprile 2008), come:
 - la policy sulla Trasparenza delle Operazioni e dei Servizi Bancari e Finanziari;
 - la procedura per la gestione dei casi di vulnerabilità dei clienti;
 - il manuale del credito per l'erogazione di prestiti personali;
 - le procedure di antiriciclaggio e lotta al finanziamento del terrorismo;
 - la gestione di vertenze legali e reclami da parte della clientela.
- controllare le funzioni centrali di supporto (incluse le attività relative Sede Secondaria)
- revisione dei controlli effettuati dalla Sede Secondaria
- rispetto da parte della Sede Secondaria degli obblighi di reportistica in ambito normativo verso la Casa Madre.

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 macro-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 presente 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 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 nell'anno a seguire, dettagliando:

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

Alla redazione del piano partecipano il dipartimento General Counsel Italy, previa condivisione con il rappresentante legale della Succursale. Tale piano viene successivamente condiviso con l'ufficio di controlli interni della Casa Madre, che potrà proporre modifiche o revisioni in ottica di un miglior allineamento della strategia di gruppo.

Una volta validato 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 atteso dal suo ufficio.

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

Per le prime si fa riferimento ai cosiddetti **controlli di primo livello** e sono essenzialmente gestiti sotto la supervisione dei manager di linea, i quali seguendo le linee guida dettate dal piano annuale di controlli interni svolgono una serie di verifiche ad hoc sulla propria area per verificare la completa aderenza alla normativa di processo in vigore. Tali controlli sono poi comunicati all'ufficio di controllo interno che li archivia e, quando previsto o necessario, li utilizza per eseguire i controlli di secondo livello.

Nei controlli a scadenza trimestrale ed annuale rientrano invece i cosiddetti controlli di secondo livello eseguiti dalla funzione incaricata allo svolgimento

dei controlli interni della Sede Secondaria nell'assetto attuale incardinati presso la struttura General Counsel Italy.

Questi controlli mirano all'analisi della conformità alla normativa e dell'adeguatezza del processo di una singola attività, selezionata appunto dall'ufficio in fase di redazione di piano annuale. La decisione di effettuare controlli trimestrali o annuali è funzione della criticità dell'attività per la quale si effettua il controllo.

Il risultato dei controlli di primo livello sono dei giudizi o commenti sulle evidenze emerse dal controllo e su criticità rilevate dal manager che ha effettuato il controllo.

I controlli di secondo livello invece portano all'emissione di una serie di raccomandazioni dell'ufficio controlli interni all'ufficio oggetto del controllo: raccomandazioni da implementare necessariamente entro la scadenza definita dall'ufficio controlli interni. 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.

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 (cfr. infra paragrafo 2.6.2), 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:

- Key Account Management
- 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 di matrici di rischio, condivise con l'intervistato, che evidenziano: le attività svolte dalle singole unità organizzative, le altre unità /funzioni aziendali e gli organi sociali a vario titolo coinvolti, i profili di rischio – ossia l'indicazione dei potenziali Reati – e l'esemplificazione delle possibili modalità di realizzazione dei Reati stessi, nonché, infine, i presidi di controllo atti a prevenire la commissione degli stessi.

Con riferimento ai presidi organizzativi, di controllo e comportamento esistenti rispetto alle specifiche fattispecie di Reato, è stata condotta una valutazione della loro idoneità a prevenire i rischi individuati evidenziando, se ritenuto opportuno, le azioni di miglioramento da apportare.

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.

E' 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, 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 fattispecie di reato di cui:

- 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.

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 proporre l'aggiornamento.

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.

Sulla base di questo presupposto e delle indicazioni contenute nelle linee guida ABI e Confindustria, gli Organi Dirigenti della Sede Secondaria hanno ritenuto opportuno, per svolgere il ruolo di OdV, individuare un organo collegiale, con sistema di voto capitaro, costituito da un membro interno e un membro esterno all'organico della Younited.

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 hanno identificato un OdV in composizione collegiale.

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 della 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.

E' 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 degli 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,
 - per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267 (legge fallimentare);
 - 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 assesment 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 4.6 "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.

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 di¹:

- *segnalazioni* relative a violazioni, presunte o effettive, del Modello;
- *segnalazioni di attività illecite* rilevanti ai sensi del D.Lgs. 231/2001 *da parte di un collaboratore⁷ o un dipendente che ne sia venuto a conoscenza per ragioni di lavoro* (il cosiddetto **Whistleblowing**), (congiuntamente con le segnalazioni di cui precedente punto, le "**Segnalazioni**"⁶);
- *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 Segnalazioni dovranno essere inviate attraverso gli specifici canali di segnalazione predisposti dalla Banca ai sensi del Decreto Legislativo nr. 10 marzo 2023, n. 24, cd. **Decreto Whistleblowing** - con cui è stata data attuazione nell'ordinamento giuridico italiano alla Direttiva "*Whistleblower*" UE 2019/1937 - ed espressamente disciplinati dalla Whistleblowing Policy adottata dalla Succursale la quale, nel recepire le disposizioni del D.Lgs. 24/2023 e Line Guida dell'ANAC emanate in data 12/07/2023, prevede i

⁶ Il Decreto Whistleblowing ha esteso l'ambito oggetto dei fatti costituenti l'oggetto della segnalazione la quale, dunque, può avere ad oggetto comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità della società, illeciti lesivi del Diritto dell'Unione Europea e condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231

seguenti canali per l'invio di una segnalazione in materia di "Whistleblowing":

a) Canale di segnalazione interno scritto e orale:

- mediante invio della Segnalazione all'indirizzo email 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);
- mediante l'utilizzo di una piattaforma informatica accessibile dalla sezione dedicata al "Whistleblowing" presente sul sito internet della Società, sia ai dipendenti che ai collaboratori esterni della Succursale, la quale 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 e, altresì, offre la possibilità di: i) inviare una Segnalazione in forma orale, procedendo con la registrazione secondo le istruzioni presenti nella piattaforma medesima e ii) richiedere un incontro con il soggetto preposto alla gestione delle segnalazioni interne.

I soggetti incaricati di ricevere le Segnalazioni (RCCI e Financial Director) all'indirizzo e-mail lanceurdalerte@younited-credit.fr, qualora i fatti oggetto di Segnalazione siano rilevanti ai sensi del presente Modello, procederanno tempestivamente a informare l'OdV della presentazione di una Segnalazione trasmettendo le informazioni e la documentazione pertinente.

b) Canale di segnalazione esterno:

- Mediante il ricorso alla piattaforma online resa disponibile dall'Autorità Nazionale Anticorruzione (ANAC) e/o l'utilizzo dello strumento della divulgazione pubblica al ricorrere di una delle condizioni espressamente previsti dalla Whistleblowing Policy a cui integralmente si rinvia

Affinché l'OdV abbia accesso al maggior numero possibile di informazioni, la Sede Secondaria garantisce la tutela di qualunque segnalante (c.d. "Whistleblower"⁷) 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 (si rimanda sul tema al successivo paragrafo 4.7).

⁷ Il Decreto Whistleblowing fornisce una definizione puntuale di "Whistleblower" per il quale si intende "la persona che segnala, divulga ovvero denuncia all'Autorità giudiziaria o contabile, violazioni di disposizioni normative nazionali o dell'Unione europea che ledono

l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato".

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 – tramite il RCCI e il Financial Director – 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.

Attraverso i canali di segnalazione interna previsti dalla Whistleblowing Policy, è consentito, altresì, l'invio di segnalazioni interne da parte di dipendenti o di persone in posizione comparabile, relative a potenziali o effettive violazioni in tema di contrasto al riciclaggio e al finanziamento del terrorismo, anche ai fini della potenziale configurabilità di commissione dei reati presupposto ex articolo 25-octies del D.Lgs. 231/2001.

In tal senso, l'Organismo di Vigilanza, per mezzo della Funzione Compliance, il cui responsabile coincide con il General Counsel Italy è direttamente informato del contenuto delle segnalazioni attraverso le modalità, previste dalla Whistleblowing Policy, le quali:

- garantiscono la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni;
- stabiliscono che il canale utilizzato per la segnalazione sia anonimo e indipendente;

- tutelano il segnalante da potenziali condotte ritorsive, discriminatorie o comunque sleali;
- lasciano all'Organo di Controllo la valutazione circa la comunicazione di quanto pervenuto ai sensi della segnalazione al Delegato per la segnalazione di operazioni sospette della Banca e/o alle Autorità di Vigilanza ai sensi dell'articolo 46 del D.Lgs. 231/2007 (così come modificato dal D.Lgs. 90/2017).

In linea con quanto previsto dalla normativa relativamente ai requisiti dei modelli di organizzazione e gestione dell'ente è inoltre previsto che:

- le segnalazioni devono basarsi su elementi di fatto che siano "precisi e concordanti";
- eventuali segnalazioni che dovessero ritenersi infondate per dolo o colpa grave del segnalante sono sanzionate;
- adozione di altre misure al fine di maggior tutela del segnalante (ad es. eventuali mutamenti di mansioni o comportamenti discriminatori connessi a segnalazioni sono nulli).

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 a seguito di specifica informativa ricevuta dal General Counsel Italy o del Membro interno dell'OdV) 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.

Si rimanda a quanto al paragrafo 4.8 *conservazione delle informazioni*, descritto di seguito, per maggiori dettagli circa i termini di archiviazione e gli altri requisiti dell'archivio previsti.

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 titolo 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 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 dell'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 neo-assunti, 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.

E' 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:

- 1 comportamenti che integrino, direttamente o indirettamente, le fattispecie di reato contemplate nel Decreto;
- 2 comportamenti che, sebbene non configurino uno dei Reati, siano inequivocabilmente strumentali alla relativa commissione;
- 3 comportamenti non conformi alle procedure delineate dal Modello, volte a ridurre il rischio di commissione di uno dei Reati;
- 4 comportamenti non conformi alle disposizioni previste nel Modello o richiamate dallo stesso e, in particolare dalle relative Parti Speciali;
- 5 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;
- 6 violazione degli obblighi di informazione verso l’OdV indicati nel paragrafo 4.6 della Parte Generale.

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.

Qualsiasi tipo di violazione delle regole comportamentali contenute nel Modello autorizza l'OdV a richiedere al soggetto titolare del potere disciplinare della Sede Secondaria, l'irrogazione di una sanzione disciplinare, determinata sulla base della gravità della violazione commessa 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.

La gravità delle violazioni del Modello sarà valutata sulla base delle seguenti circostanze:

- la presenza e l'intensità dell'elemento intenzionale;
- la presenza e intensità della condotta negligente, imprudente, imperita;
- la presenza e intensità della condotta recidiva;
- l'entità del pericolo e/o delle conseguenze della violazione per la Sede Secondaria;
- l'entità del pericolo e/o delle conseguenze della violazione per le persone destinatarie della normativa in materia di tutela della salute e della sicurezza sui luoghi di lavoro, nonché per la Sede Secondaria;
- la prevedibilità delle conseguenze della condotta in violazione;
- i tempi e i modi della violazione;
- le circostanze nelle quali la violazione ha avuto luogo.

6.2. Misure nei confronti dei dipendenti

La violazione delle singole regole comportamentali di cui al presente Modello da parte dei dipendenti della Sede Secondaria italiana soggetti al CCNL per il settore del commercio per i dipendenti da aziende del terziario, della distribuzione e dei servizi – Confcommercio (30 luglio 2019) . costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori - nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili - sono quelli previsti dall'apparato sanzionatorio di cui al suddetto CCNL, e precisamente (art. 22):

- a. biasimo inflitto verbalmente per le mancanze più lievi;
- b. biasimo inflitto per iscritto nei casi di recidiva;
- c. multa in misura non eccedente l'importo di mezza giornata di retribuzione;

- d. sospensione dalla retribuzione e dal servizio per un massimo di 10 giorni;
- e. licenziamento disciplinare, senza preavviso e con altre conseguenze di ragione e di legge (licenziamento in tronco).

Quando sia richiesto dalla natura della mancanza o dalla necessità di accertamenti in conseguenza della medesima, la Sede Secondaria - in attesa di deliberare il definitivo provvedimento disciplinare - può disporre l'allontanamento temporaneo del lavoratore/lavoratrice dal servizio per il tempo strettamente necessario.

In ogni caso, delle sanzioni irrogate e/o delle violazioni accertate, la funzione aziendale competente terrà sempre informato l'OdV delle sanzioni irrogate e/o delle violazioni accertate.

In particolare, con riferimento alle violazioni del Modello poste in essere dai dipendenti di Younited, si prevede che:

1. incorre nei provvedimenti di **biasimo verbale o scritto** secondo la gravità della violazione, il dipendente che violi le procedure interne previste dal presente Modello o adottati, nell'espletamento di attività nei Processi a Rischio, un comportamento in violazione delle prescrizioni del Modello stesso, purché tale condotta non imponga l'applicazione di misure previste dal Decreto;
2. incorre nel provvedimento di **sospensione dalla retribuzione e dal servizio per un massimo di dieci giorni** il dipendente che nel violare le procedure interne previste dal presente Modello o adottando nell'espletamento di attività nelle Processi a rischio un comportamento in violazione delle prescrizioni dello stesso, arrechi danno alla Sede Secondaria o esponga l'integrità dei beni della stessa a una situazione di pericolo, purché tali condotte non siano comunque dirette in modo univoco alla commissione di un Reato o non determinino l'applicazione di misure previste dal Decreto;
3. incorre nel provvedimento di **licenziamento in tronco a seconda della gravità della violazione ai sensi dell'art. 22 del CCNL** il dipendente che adotti un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, nonché il dipendente che adotti un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico della Sede Secondaria di misure previste dal Decreto.

Inoltre, con specifico riferimento alle violazioni delle prescrizioni del Modello previste in materia di **tutela della salute e della sicurezza sui luoghi di lavoro**:

1. incorre nel provvedimento di **sospensione dalla retribuzione e dal servizio per un massimo di dieci giorni** il dipendente che, nel violare le procedure interne previste dal presente Modello in materia di tutela della salute e della sicurezza sui luoghi di lavoro, abbia adottato un comportamento in violazione alle prescrizioni del Modello stesso determinando un rilevante rischio differenziale⁸ tale da esporre la Sede Secondaria ad un più grave rischio di applicazione di misure previste dal Decreto (trattasi, ad esempio, di condotta negligente, imperita od imprudente del lavoratore durante le attività di formazione e addestramento);
2. incorre nel provvedimento del **licenziamento in tronco a seconda della gravità della violazione ai sensi dell'art. 22 del CCNL** il lavoratore che adotti un comportamento in violazione alle prescrizioni del presente Modello tale da esporre la Sede Secondaria al rischio concreto ed immediato di applicazione di misure previste dal Decreto (trattasi, a mero titolo esemplificativo, di condotta negligente, imprudente od imperita suscettibile di provocare un infortunio a sé stesso ovvero ad altre persone).

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 6.1 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:

⁸ Con specifico riferimento alle violazioni a prescrizioni del Modello previste in materia di tutela della salute e della sicurezza sui luoghi di lavoro, si precisa che per "rischio differenziale" si deve intendere il margine di rischio ulteriore rispetto a quello già individuato in sede di valutazione dei rischi da parte della Sede Secondaria e derivante dal comportamento del lavoratore.

- 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.

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

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, 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.

Ai fini del presente documento si intendono per "Pubblica Amministrazione", in via esemplificativa⁹:

- 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 autoritativi¹⁰ o certificativi¹¹, 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,

⁹ L'elenco delle Amministrazioni Pubbliche previsto dalla legge n. 311 del 30/12/2004 pubblicato annualmente dall'ISTAT, può essere reperito nel sito internet dell'ISTAT all'indirizzo www.istat.it Strumenti -> definizioni e classificazioni -> elenco delle amministrazioni pubbliche.

¹⁰Rientra nel concetto di "poteri autoritativi" non solo il potere di coercizione ma ogni attività discrezionale svolta nei confronti di soggetti che si trovano su un piano non paritetico rispetto all'autorità (cfr. Cass., Sez. Un. 11/07/1992, n. 181).

¹¹Rientrano nel concetto di "poteri certificativi" tutte quelle attività di documentazione cui l'ordinamento assegna efficacia probatoria, quale che ne sia il grado.

- 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..

3.2. 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..

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.

A titolo meramente esemplificativo si possono menzionare i seguenti soggetti, nei quali la giurisprudenza ha individuato la qualifica di Pubblico Ufficiale: ufficiale giudiziario, consulente tecnico del giudice, curatore fallimentare, esattore o dirigente di aziende municipalizzate anche se in forma di S.p.A., assistente universitario, portalettere, funzionario degli uffici periferici dell'Automobil Club d'Italia (ACI), consigliere comunale, geometra tecnico comunale, insegnante delle scuole pubbliche, ufficiale sanitario, notaio, dipendente dell'Istituto Nazionale della Previdenza Sociale (INPS), medico convenzionato con l'Azienda Sanitaria Locale, tabaccaio che riscuote le tasse automobilistiche.

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

¹²Rientra nel concetto di poteri autoritativi non solo il potere di coercizione ma ogni attività discrezionale svolta nei confronti di soggetti che si trovano su un piano non paritetico rispetto all'autorità (cfr. Cass., Sez. Un. 11/07/1992, n.181). I poteri certificativi comprendono tutte quelle attività di documentazione cui l'ordinamento assegna efficacia probatoria, quale che ne sia il grado.

giurisprudenza ha individuato la qualifica di Incaricato di Pubblico Servizio: esattori dell'Enel, lettori 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 riguarda: 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.

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, dopo avere ricevuto in modo lecito finanziamenti, sovvenzioni o contributi da parte dello Stato italiano o delle Comunità Europee per la realizzazione di opere o attività di interesse pubblico, non si proceda all'utilizzo delle somme per le finalità per cui sono state concesse.

Il delitto si consuma anche se solo una parte dei fondi viene distratta e anche nel caso in cui la parte correttamente impiegata abbia esaurito l'opera o l'iniziativa cui l'intera somma era destinata.

La condotta criminosa prescinde dal modo in cui sono stati ottenuti i fondi e si realizza solo in un momento successivo all'ottenimento dei fondi stessi.

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. A nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato si perfeziona nel momento dell'ottenimento dei finanziamenti.

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.)

Parte attiva del reato di concussione può essere il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio che, abusando della sua qualità o dei suoi poteri, costringa taluno a dare o a promettere a lui o a un terzo denaro o altre utilità non dovute.

La costrizione si attua mediante violenza o minaccia di un danno ingiusto (ad esempio: rifiuto di compiere un atto dovuto se non contro compenso), con modalità tali da non lasciare libertà di scelta alla persona che la subisce,

la quale è considerata vittima del reato e quindi esente da pena. Pertanto, la responsabilità degli enti a titolo di concussione 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 estorsiva posta in essere in concorso con un Pubblico Ufficiale o un Incaricato di Pubblico Servizio nei confronti di un terzo;
- condotta estorsiva 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.

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.)

In questa fattispecie di reato la condotta del corrotto e del corruttore è caratterizzata dal fine specifico di favorire o di danneggiare una parte in un processo penale, civile o amministrativo.

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.

¹³ L'art. 318 c.p. previgente alla "legge anticorruzione" contemplava la sola ipotesi della cosiddetta "corruzione impropria", vale a dire l'indebito compenso per il compimento di uno specifico atto, dovuto o comunque conforme ai doveri d'ufficio, del pubblico agente. Il comma 2 prevedeva la condotta di "corruzione impropria susseguente", vale a dire l'indebito compenso non pattuito, ma corrisposto dopo il compimento di un atto d'ufficio, ipotesi in cui era punito il corrotto, ma non il corruttore. A seguito dell'abolizione di tale comma, anche la condotta predetta rientra nella formulazione del comma 1, con la conseguenza che ora sono puniti entrambi anche in tale caso (cfr. l'art. 321 c. p.). Infine, non ha più rilevanza la qualità di dipendente pubblico dell'incaricato di pubblico servizio, che era richiesta per la sussistenza del reato in questione.

Traffico di influenze illecite (art. 346-bis c.p.)¹⁴

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 prefigurino 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.

3.3. 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:

- Stipula dei rapporti contrattuali con la Pubblica Amministrazione;
- Gestione dei rapporti contrattuali con la Pubblica Amministrazione;
- Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione della formazione finanziata;
- Gestione e utilizzo dei sistemi informativi e del Patrimonio Informativo della Società;

¹⁴ 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.

- Gestione dei contenziosi e degli accordi transattivi;
- Gestione dei rapporti con le Autorità di Vigilanza;
- 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 del patrimonio immobiliare;
- Gestione dei rapporti con i Regolatori.

Con riferimento all'attività sensibile concernente la Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Younited si rimanda al protocollo 8.3.1;

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 regola 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.

3.3.1 Gestione dei rapporti contrattuali con la Pubblica Amministrazione

Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione di rapporti contrattuali con gli Enti della Pubblica Amministrazione.

Ai sensi del D. Lgs n. 231/2001, i relativi processi potrebbero presentare occasioni per la commissione dei reati di "corruzione", nelle loro varie tipologie, di "induzione indebita a dare o promettere utilità", di "traffico di influenze illecite"¹⁵, di "concussione" e di "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.

Descrizione dei processi

¹⁵ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all'induzione indebita 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 riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi delle Comunità Europee, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

Il processo di gestione del rapporto contrattuale di servizio di gestione di portafogli si articola nelle seguenti fasi:

- analisi preliminare dei presupposti per l'esecuzione del contratto (es. definizione delle caratteristiche della gestione);
- esecuzione del contratto;
- monitoraggio sull'esecuzione del contratto e rendicontazione alla clientela.

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.

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 con i Funzionari pubblici in costanza di esecuzione degli obblighi di natura contrattuale con gli Enti stessi è organizzativamente demandata a specifiche strutture della Sede Secondaria che si occupano della erogazione di prodotti / servizi oggetto del contratto. La stipula dei contratti per l'esecuzione di servizi nei confronti della Pubblica Amministrazione è effettuata nel rispetto dei principi di comportamento sanciti dal Protocollo per la "Stipula dei rapporti contrattuali con la Pubblica Amministrazione" e, in particolare, tutti gli atti che impegnano contrattualmente la Sede Secondaria nei confronti di terzi devono essere sottoscritti soltanto da soggetti appositamente incaricati;
- nell'ambito di ogni struttura, i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione dei rapporti contrattuali con la Pubblica Amministrazione:
 - sono individuati e 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;
 - operano esclusivamente nell'ambito del perimetro di clientela loro assegnato dal Responsabile della Struttura di riferimento;
 - sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.
- Segregazione dei compiti tra i soggetti coinvolti nel processo di gestione degli accordi contrattuali con gli Enti pubblici. In particolare:
 - i soggetti deputati alla predisposizione della documentazione per la rendicontazione agli enti sono differenti da coloro che

- sottoscrivono la stessa;
- le Strutture incaricate della gestione operativa dei prodotti/servizi contrattualizzati, sono diverse da quelle incaricate dello sviluppo commerciale.
 - Attività di controllo: la normativa interna di riferimento identifica i controlli di linea che devono essere svolti a cura di ciascuna Struttura interessata nello svolgimento delle attività di natura contabile/amministrativa inerenti all'esecuzione dei processi oggetto del presente protocollo. In particolare dovrà essere assicurata la verifica della regolarità delle operazioni nonché della completezza, della correttezza e della tempestività delle scritture contabili che devono essere costantemente supportate da meccanismi di maker e checker.
 - Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - la realizzazione delle operazioni nella esecuzione degli adempimenti contrattuali verso la Pubblica Amministrazione prevede l'utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate. Le strutture provvedono alla archiviazione della documentazione cartacea inerente all'esecuzione degli adempimenti svolti;
 - ciascuna Struttura di volta in volta interessata, al fine di consentire la ricostruzione delle responsabilità, 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 delle attività proprie del processo della gestione dei rapporti con la Pubblica Amministrazione.
 - 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.

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 segnalare 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 secondo quanto previsto dal paragrafo 4.6.;
- 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.

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

Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione delle attività inerenti alla richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione quali, a titolo esemplificativo e non esaustivo:

- gestione dei rapporti con gli Enti assistenziali e previdenziali e realizzazione, nei tempi e nei modi previsti, degli adempimenti di legge in materia di lavoro e previdenza (INPS, INAIL, Direzione Provinciale del Lavoro, Medicina del Lavoro, Agenzia delle Entrate, Enti pubblici locali, ecc.);
- gestione dei rapporti con gli Enti Locali per l'esecuzione delle attività inerenti al registro delle imprese;
- gestione dei rapporti con Amministrazioni Statali, Regionali, Comunali o Enti locali (A.S.L., Vigili del Fuoco, Arpa, etc.) per l'esecuzione di adempimenti in materia di igiene e sicurezza e/o di autorizzazioni (ad esempio pratiche edilizie), permessi, concessioni;
- gestione dei rapporti con il Ministero dell'Economia e delle Finanze, con le Agenzie Fiscali e con gli Enti pubblici locali per l'esecuzione di adempimenti in materia di imposte;
- gestione dei rapporti con Banca d'Italia per l'esecuzione degli adempimenti in materia di mantenimento della riserva obbligatoria;

- gestione dei rapporti con la Prefettura, la Procura della Repubblica e le Camere di Commercio competenti per la richiesta di certificati e autorizzazioni;
- gestione degli accertamenti bancari.

Ai sensi del D. Lgs n. 231/2001, le predette attività potrebbero presentare occasioni per la commissione dei reati di “corruzione”, nelle loro varie tipologie, di “induzione indebita a dare o promettere utilità”, di “traffico di influenze illecite”¹⁶ e di “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.

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.

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - nell’ambito di ogni Struttura, tutti i soggetti che intervengono nella gestione delle attività inerenti alla richiesta di autorizzazioni alla Pubblica Amministrazione:
 - sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile della Struttura di riferimento

¹⁶Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all’induzione indebita 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 riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni o degli organi delle Comunità Europee, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali

- tramite delega interna, da conservare a cura della Struttura medesima; nel caso in cui i rapporti con gli Enti pubblici vengano intrattenuti da soggetti terzi, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali;
- operano esclusivamente nell'ambito del perimetro di clientela loro assegnato dal Responsabile della Struttura di riferimento;
 - la gestione dei rapporti con i Funzionari pubblici in caso di accertamenti/sopralluoghi, effettuati anche allo scopo di verificare l'ottemperanza alle disposizioni di legge che regolamentano l'operatività dell'area di propria competenza, 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 la Pubblica Amministrazione 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 dell'istanza di autorizzazione o forniti in esecuzione degli adempimenti, prevedendo, ove opportuno, specifici controlli in contraddittorio. In particolare, laddove l'autorizzazione/adempimento preveda l'elaborazione di dati ai fini della predisposizione dei documenti richiesti dall'Ente pubblico, 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 all'Ente pubblico per la richiesta di autorizzazione o per l'esecuzione di adempimenti è conservata presso l'archivio della struttura di competenza;
 - il Responsabile della Struttura, ovvero il soggetto aziendale all'uopo incaricato ha l'obbligo di firmare per accettazione il verbale redatto dai Funzionari pubblici in occasione degli accertamenti/sopralluoghi condotti presso la Sede Secondaria e di mantenerne copia nei propri uffici, 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 alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla richiesta di autorizzazioni alla Pubblica Amministrazione.

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 segnalare 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 secondo quanto previsto dal paragrafo 4.6.;
- 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.

3.3.3 Gestione della formazione finanziata

Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione della formazione finanziata.

Attraverso la gestione della formazione finanziata la Sede Secondaria, laddove sussistano i presupposti, usufruisce dei 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 quelli concessi a valere su:

- 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);
- F.B.A. (Fondo Banche e Assicurazioni);

- Fondo di solidarietà per il sostegno del reddito, dell'occupazione e della riconversione e riqualificazione professionale del personale del credito.

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”*, di *“traffico di influenze illecite”*¹⁷, di *“truffa aggravata per il conseguimento di erogazioni pubbliche”*, di *“malversazione”* e di *“indebita percezione di erogazioni a danno dello Stato”*.

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.

Descrizione del processo

Il processo si articola nelle seguenti fasi:

- individuazione iniziative finanziabili;
- predisposizione e presentazione della richiesta di finanziamento/contributo all'Ente pubblico, corredata, laddove previsto, dal verbale di accordo sottoscritto con le competenti OO.SS.LL.;
- attuazione dei progetti finanziati;
- gestione dell'operatività dell'iniziativa finanziata;
- gestione delle risorse previste dal progetto/iniziativa (economiche e tecniche, interne ed esterne);
- rendicontazione dei costi;
- raccolta dei dati contabili, elaborazione e stesura di *report*;
- gestione dei rapporti con Enti in occasione di verifiche e ispezioni da parte dell'Ente finanziatore;
- gestione dell'introito del contributo.

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

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:

¹⁷ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all'induzione indebita 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, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

- tutti i soggetti che, nell'ambito della "gestione della formazione finanziata", esercitano poteri autorizzativi e/o negoziali nei rapporti con gli Enti finanziatori:
 - 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;
 - operano esclusivamente nell'ambito del perimetro loro assegnato dal Responsabile della Struttura di riferimento;
- le richieste di finanziamento/contributo sono sottoscritte dal Responsabile della Struttura competente specificamente e formalmente facoltizzato in virtù del vigente sistema dei poteri e delle deleghe; la normativa interna illustra tali meccanismi autorizzativi, fornendo le indicazioni dei soggetti aziendali cui sono attribuiti i necessari poteri.
- in caso di eventuale ricorso a consulenti esterni, il processo di attribuzione dell'incarico avviene uniformemente a quanto previsto dalle disposizioni contenute nella specifica sezione dedicata nel presente Modello (protocollo per "*la gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali*"). La selezione di tali consulenti avviene in ogni caso prevedendo l'acquisizione di una pluralità di offerte e la scelta mediante criteri oggettivi e codificati.
- Segregazione dei compiti tra i soggetti coinvolti, volta a garantire, per tutte le fasi del processo, un meccanismo di *maker* e *checker*. In particolare, la Struttura competente attribuisce a ciascun ufficio organizzativamente dipendente, in funzione dei ruoli ricoperti da ciascun addetto, le attività operative e le attività di controllo da effettuare al fine di garantire la contrapposizione di ruoli tra i soggetti che gestiscono le fasi istruttorie del processo della formazione finanziata ed i soggetti deputati alle attività di verifica.
- Attività di controllo da parte di ciascuna Struttura competente della Sede Secondaria ed in particolare:
 - verifica della coerenza dei contenuti del progetto di formazione rispetto a quanto disposto dalle direttive del bando di finanziamento;
 - verifica della regolarità formale della documentazione da consegnare all'Ente per l'accesso al bando di finanziamento;
 - tenuta del registro presenze durante l'erogazione dei progetti formativi e utilizzo di sistemi informatici di supporto per la gestione del personale, in cui sono registrate tutte le informazioni relative alle presenze ed alle attività svolte;
 - puntuale attività di controllo sul processo di rendicontazione delle spese, attraverso:

- raccolta e verifica dei registri di presenza compilati in ogni loro parte dai partecipanti agli interventi formativi;
 - raccolta della documentazione degli oneri aziendali dei dipendenti partecipanti / docenti, sulla base del corrispettivo orario calcolato a cura dell'ufficio competente in considerazione delle matricole che hanno partecipato all'iniziativa;
 - raccolta e verifica delle parcelle/fatture relative ai costi sostenuti per l'iniziativa;
 - verifica sulla puntuale e corretta contabilizzazione degli introiti.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali: tutte le fasi di processo sono documentate, così come previsto dagli stessi bandi per l'ottenimento dei finanziamenti.
- In particolare, ciascuna Struttura coinvolta nell'ambito del processo della formazione finanziata, è responsabile dell'archiviazione e della conservazione della documentazione di propria competenza, ivi inclusa quella trasmessa all'Ente finanziatore pubblico anche in via telematica o elettronica.

Principi di comportamento

Le Strutture a qualsiasi titolo coinvolte nella attività di gestione della formazione finanziata 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:

- 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 che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Younited (es.: pratiche di richiesta, studi di fattibilità, piani di progetto, ecc.) 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 secondo quanto previsto dal paragrafo 4.6.;
- qualora sia previsto il coinvolgimento di soggetti terzi nella predisposizione delle pratiche di richiesta / gestione del finanziamento o nella successiva esecuzione di attività connesse con

i programmi finanziati, 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 e alterati;
- tenere una condotta ingannevole che possa indurre gli Enti finanziatori/erogatori in errore di valutazione tecnico-economica della documentazione presentata;
- 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 decisione di accoglimento delle domande di ammissione al contributo;
- destinare contributi, sovvenzioni, finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti;
- 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 nell'ottenimento di contributi. 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 finanziarie che comportino la generazione di una perdita per la Sede Secondaria e la creazione di un utile per i soggetti predetti;
- 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 alla Pubblica Amministrazione e dalla conseguente possibilità di facilitare/velocizzare l'iter istruttorio delle pratiche.

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.

I principi di comportamento illustrati nel presente protocollo devono intendersi altresì estesi, per quanto compatibili, ad ogni eventuale ulteriore processo aziendale concernente la richiesta e la gestione di contributi/incentivi pubblici a favore della Sede Secondaria concessi a qualsiasi altro titolo.

3.3.4 Gestione dei contenziosi e degli accordi transattivi

Premessa

Il presente protocollo si applica a tutte le Strutture della Sede Secondaria coinvolte nella gestione dei contenziosi giudiziari 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. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "*corruzione*", nelle loro varie tipologie¹⁸, di "*induzione indebita a dare o promettere utilità*", di "*traffico di influenze illecite*"¹⁹ e di "*truffa ai danni dello Stato o di altro ente pubblico*" nonché del reato di "*induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*"²⁰.

Sussiste altresì il rischio della commissione del reato di "*corruzione tra privati*" e di "*istigazione alla corruzione tra privati*", descritti nel paragrafo 4.2. 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.

Descrizione del Processo

Il processo di gestione del contenzioso si articola nelle seguenti fasi,

¹⁸ Ivi compresa la "*Corruzione in atti giudiziari*" (art. 319-ter comma 1, c.p.).

¹⁹ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all'induzione indebita 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, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

²⁰ Tale reato, punito dall'art. 377-bis c.p. costituisce reato presupposto della responsabilità degli enti ai sensi dell'art. 25-novies del Decreto. Inoltre, ai sensi dell'art. 10 della L. n.146/2006 può dar luogo alla medesima responsabilità anche se commesso in forma transazionale. Si considera reato transazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

- sia commesso in più di uno Stato;
- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero sia commesso in uno Stato, ma abbia effetti sostanziali in un altro Stato".

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.

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.

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 secondo quanto previsto dal paragrafo 4.6.

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 utilità²¹, - a tacere o a

21 intendendosi per "altre utilità": doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) ovvero vantaggi di qualsiasi natura da accordare al Funzionario pubblico italiano o straniero a titolo personale 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 e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Sede secondaria e la

- 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.

creazione di un utile per il pubblico ufficiale (es. applicazioni di condizioni non in linea con i parametri di mercato).

3.3.5 Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali

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 creativo²², 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"²³.

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 "tributarî", descritti nel paragrafo 10.2.

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"²⁴, 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.

Descrizione del Processo

L'attività di gestione delle procedure acquisitive dei beni e dei servizi si

²² Ai sensi dell'art. 2575 del codice civile, le opere dell'ingegno di carattere creativo tutelate dal diritto d'autore sono quelle che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì considerate e protette come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale ne costituiscono una creazione intellettuale dell'autore (art. 1 L. 22 aprile 1941, n. 633).

²³ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all'induzione 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 riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi delle Comunità Europee, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

²⁴ Si vedano al riguardo il paragrafo 7.4 e il paragrafo 7.9.

articola nei seguenti processi:

- definizione e gestione del *budget*;
- gestione degli approvvigionamenti;
- gestione del ciclo passivo;
- gestione dei fornitori.

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

Principi di controllo

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

- Livelli autorizzativi definiti:
 - 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;
 - la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati in base a criteri individuati nell'ambito della normativa interna, fatte salve esigenze/forniture occasionali. Tali soggetti devono garantire e su richiesta poter documentare anche con riferimento ai subappaltatori da loro incaricati:
 - in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi – il rispetto della disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti;
 - in relazione ai lavoratori impiegati, il rispetto della disciplina in tema di immigrazione e la regolarità retributiva, contributiva, previdenziale, assicurativa e fiscale;
 - l'eventuale affidamento a terzi - da parte dei fornitori della Sede Secondaria- di attività in sub-appalto, è contrattualmente subordinato ad un preventivo assenso da parte della struttura della Sede Secondaria che ha stipulato il contratto;
 - l'autorizzazione al pagamento della fattura spetta ai Responsabili delle Strutture per le quali è prevista l'assegnazione di un budget e delle relative facoltà di spesa (Centri di Responsabilità) o ai soggetti all'uopo incaricati; può essere negata a seguito di formale contestazione delle

- inadempienze/carenze della fornitura adeguatamente documentata e dettagliata a cura delle predette Strutture;
- il pagamento delle fatture è effettuato da una specifica Struttura aziendale dedicata.
 - Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle procedure acquisitive. In particolare:
 - le attività di cui alle diverse fasi del processo devono essere svolte da soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di *maker e checker*.
 - Attività di controllo: la normativa interna di riferimento identifica i controlli che devono essere svolti a cura di ciascuna Struttura interessata in ogni singola fase del processo:
 - 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 individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti (l'avvio della relazione deve essere preceduta da un'adeguata due diligence);
 - verifica del rispetto delle norme di legge che vietano o subordinano a determinate condizioni il conferimento di incarichi di qualunque tipologia a dipendenti pubblici o ex dipendenti pubblici.

Per quanto concerne infine il conferimento di incarichi professionali e consulenze il cui svolgimento comporta un rapporto diretto con la Pubblica Amministrazione (quali ad esempio spese legali per contenzioso, onorari a professionisti per pratiche edilizie, spese per consulenze propedeutiche all'acquisizione di contributi pubblici, ecc.) i Responsabili delle Strutture interessate dovranno:

- disporre che venga regolarmente tenuto in evidenza l'elenco dei professionisti/consulenti, l'oggetto dell'incarico ed il relativo corrispettivo;
- verificare periodicamente il suddetto elenco al fine di individuare eventuali situazioni anomale.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
 - documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista anche attraverso gare, in termini di motivazione della scelta nonché pertinenza e congruità della spesa. La normativa interna individua in quali casi l'individuazione del fornitore di beni e/o servizi o professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte;

- 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 alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.

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.

3.3.6 Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni

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"²⁵.

Sussiste altresì il rischio della commissione dei reati di "corruzione tra privati" e di "istigazione alla corruzione tra privati" descritti nel paragrafo 4.2. 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.

Descrizione del Processo

I processi di gestione degli omaggi e delle spese di rappresentanza hanno ad oggetto i beni destinati ad essere offerti, in qualità di cortesia commerciale, a soggetti terzi, quali, ad esempio, 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 ogni altra utilità (ad esempio inviti ad eventi sportivi, spettacoli e intrattenimenti, biglietti omaggio, etc.) provenienti o destinati al medesimo soggetto/ente, che non superino, in un anno solare, il valore di 150 euro.

I processi di gestione delle spese per beneficenze e per sponsorizzazioni si

²⁵ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore e del soggetto che cede all'induzione 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 riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi delle Comunità Europee, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

articolarono nelle seguenti fasi:

- ricezione della richiesta, inviata dagli Enti, di elargizioni e di beneficenze o sponsorizzazioni per progetti, iniziative, manifestazioni;
- individuazione di società/organizzazioni cui destinare le elargizioni;
- effettuazione delle attività di *due diligence*²⁶ della Sede Secondaria;
- esame/valutazione dell'iniziativa/progetto proposto;
- autorizzazione alla spesa e, qualora previsto, stipula dell'accordo/contratto;
- erogazione delle elargizioni da parte della Sede Secondaria.

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

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

²⁶ Ricerca di informazioni rilevanti sull'Ente richiedente quali, a titolo esemplificativo e non esaustivo denominazione, natura giuridica e data di costituzione, sulla sede legale e operativa (se diversa da quella legale) ed eventuale sito web, legale rappresentante ed eventuali notizie sulla sua reputazione, notizie sull'ente e sulle sue linee strategiche, sulla dimensione (numero dipendenti e/o collaboratori, numero di soci), sui principali progetti realizzati negli ultimi due anni nel settore di riferimento dell'iniziativa proposta, sintesi delle informazioni finanziarie relative ai bilanci approvati negli ultimi due anni, ecc.

- 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.
 - 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 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 approvate 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.
 - Inoltre i Responsabili delle Strutture interessate dovranno:
 - 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 della 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/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 alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni.

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 secondo quanto previsto dal paragrafo 4.6;
- 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.

3.3.7 Gestione del processo di selezione e assunzione del personale

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 4.2).

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.

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.

Resta nelle competenze delle Strutture aziendali specificatamente facoltizzate l’istruttoria relativa alla selezione ed assunzione di personale specialistico altamente qualificato ovvero di figure destinate a posizioni di vertice (cosiddetta “assunzione a chiamata”).

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.

Principi di controllo

²⁷ Si ricorda che, ai sensi dell’art. 322-bis c.p., la condotta del corruttore e del soggetto che cede all’induzione 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 riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni o degli organi delle Comunità Europee, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

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

- Livelli autorizzativi definiti:
 - accentramento del processo di selezione e assunzione del personale in capo alla Struttura competente che riceve le richieste formali di nuovo personale da parte delle Strutture interessate e le valuta in coerenza con il budget ed i piani interni di sviluppo;
 - autorizzazione all'assunzione concessa soltanto dal personale espressamente facoltizzato secondo il vigente sistema dei poteri e delle deleghe;
 - l'assunzione dei candidati individuati come idonei e per i quali è stata fornita autorizzazione all'inserimento viene effettuata dalle Unità Organizzative competenti per Struttura.
- Segregazione dei compiti tra i diversi soggetti coinvolti nel processo. In particolare l'approvazione finale dell'assunzione è demandata a strutture diverse, commisurate all'importanza della posizione ricercata all'interno dell'organizzazione aziendale.
- Attività di controllo:
 - compilazione da parte del candidato, al momento dello svolgimento della selezione, di un'apposita modulistica per garantire la raccolta omogenea delle informazioni sui candidati;
 - l'assunzione deve essere preceduta da un'adeguata due diligence;
- 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 (tra cui quella standard ad esempio testi, *application form*, contratto di lavoro, ecc.) anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di selezione e assunzione del personale.

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 secondo quanto previsto dal paragrafo 4.6.;

- 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.

3.3.8 Gestione dei rapporti con i Regolatori

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*"²⁸.

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").

Descrizione del Processo

²⁸ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore o del soggetto che cede all'induzione indebita 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, 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 o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

Le attività inerenti la gestione dei rapporti con i Regolatori sia direttamente che mediante terzi (consulenti, associazioni di categoria, i “*think tank*”, i Gruppi di interesse) sono riconducibili alle seguenti tipologie:

- contatto con l’Ente;
- evasione di specifiche richieste / documenti di consultazione;
- produzione di specifiche istanze/*position paper*.

La Sede Secondaria gestisce direttamente i rapporti con le Autorità di Regolamentazione *Host*, informando tempestivamente la Casa Madre, a fronte di tematiche che non abbiano valenza rilevante per il Gruppo, coinvolgendo la Casa Madre per i restanti casi.

Le modalità operative per la gestione del processo sono disciplinate nell’ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti (cfr. Guida Operativa “*Gestione delle comunicazioni con le Autorità di Supervisione e di Regolamentazione*”), che costituisce parte integrante e sostanziale del presente protocollo.

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.

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 secondo quanto previsto dal paragrafo 4.6.;
- 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 preliminarmente 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. I REATI SOCIETARI

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, 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.

4.2 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 espongono 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 ostacolano 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;

Aggiotaggio (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 (2638 c.c.) - Tale reato si realizza qualora nelle comunicazioni con le autorità di vigilanza previste ai sensi della normativa applicabile si espongono 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.

Corruzione tra privati e istigazione alla corruzione tra privati, ai sensi dell'art. 25-ter del D.Lgs. 231/2001 (ex artt. 2635 c.c. e 2635-bis c.c.), – Tale fattispecie di reato si realizza, a titolo esemplificativo e non esaustivo, laddove, nell'ambito della selezione di advisors, finders o altri consulenti terzi, si favoriscano soggetti apicali ovvero soggetti che rivestono funzioni direttive di fatto in una società avente natura privatistica, – anche a seguito di induzione da parte dello stesso – pur in assenza dei necessari requisiti di

professionalità e/o convenienza economica, al fine di ottenere, in altra occasione, un vantaggio per la Banca.

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.

4.3 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.

4.3.1 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.

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 7.11 (Area sensibile concernente i reati tributari). 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.

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.

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 ed, 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 *disclosures*.

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.

5. REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO, REATI DI CRIMINALITÀ ORGANIZZATA, REATI TRANSNAZIONALI

5.1. Premessa

Attraverso ripetuti interventi legislativi sono state introdotte nel sistema della responsabilità amministrativa degli Enti varie categorie di illeciti, con la comune finalità di contrastare fenomeni di criminalità che destano particolare allarme a livello internazionale, specie in relazione a reati di matrice politico-terroristica, oppure commessi nei settori e con le forme tipiche della delinquenza organizzata, anche transnazionale, o particolarmente lesivi di fondamentali diritti umani.

Il settore finanziario ha da sempre dedicato particolare attenzione ed impegno nella collaborazione alla prevenzione di fenomeni criminali nel mercato finanziario ed al contrasto al terrorismo, impegno questo che la Younited assume anche ai fini della tutela della sana e prudente gestione, della trasparenza e correttezza dei comportamenti e del buon funzionamento del sistema nel suo complesso. Inoltre, nell'esercizio dell'attività finanziaria è di particolare evidenza il rischio di mettere a disposizione di clientela appartenente o comunque contigua alla malavita organizzata servizi o risorse finanziarie che risultino strumentali al perseguimento di attività illecite.

Si fornisce qui di seguito una sintetica esposizione delle categorie di fattispecie in questione.

5.2. Le fattispecie di reato previste dall'art. 25-*quater* del Decreto

L'art. 25-*quater* del Decreto dispone la punibilità dell'ente, ove ne sussistano i presupposti, nel caso in cui siano commessi, nell'interesse o a vantaggio dell'ente stesso, delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale, dalle leggi speciali o dalla Convenzione internazionale per la repressione del finanziamento del terrorismo, firmata a New York il 9 dicembre 1999. La norma non prevede un elenco di reati chiuso e tassativo, ma si riferisce ad un qualsivoglia illecito penale caratterizzato dalla particolare finalità di terrorismo o di eversione dell'ordine democratico perseguita dal soggetto agente²⁹.

Si menzionano qui di seguito le principali fattispecie che possono venire in considerazione.

A) Delitti con finalità di terrorismo o eversione dell'ordine democratico

²⁹ L'art. 270-sexies c.p. considera connotate da finalità di terrorismo le condotte che possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o ad astenersi dal compiere un qualsiasi atto, o di destabilizzare le strutture politiche fondamentali, costituzionali, economiche e sociali, nonché le altre condotte previste da convenzioni o da norme internazionali. Secondo la giurisprudenza (Cass. pen. n. 39504/2008) l'espressione "eversione dell'ordine democratico" non può essere limitata al solo concetto di azione politica violenta, ma deve intendersi riferita all'ordinamento costituzionale, e quindi ad ogni mezzo di lotta politica che tenda al sovvertimento del sistema democratico e costituzionale esistente o alla deviazione dai principi fondamentali che lo governano.

previsti dal codice penale o da leggi penali speciali.

Si tratta dei delitti politici, cioè contro la personalità interna ed internazionale dello Stato, contro i diritti politici del cittadino, nonché contro gli Stati esteri, i loro Capi e i loro rappresentanti.

Le fattispecie di maggior rischio sono quelle concernenti il **“Finanziamento di condotte con finalità di terrorismo”** (art. 270-quinquies.1 c.p.), la **“Sottrazione di beni o denaro sottoposti a sequestro”** (art. 270-quinquies.2 c.p.), la **“Partecipazione a prestiti a favore del nemico”** (art. 249 c.p.), il **“Sequestro di persona a scopo di terrorismo o di eversione”** (art. 289 bis c.p.) e il reato di cui all’art. 270 bis c.p., denominato **“Associazioni con finalità di terrorismo anche internazionale o di eversione dell’ordine democratico”**. In particolare, tale ultima fattispecie punisce anche qualsiasi forma di finanziamento a favore di associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione.

Si richiama inoltre l’attenzione sui reati a danno del patrimonio, ed in particolare sulle fattispecie di riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, beninteso qualora commessi strumentalmente al perseguimento di finalità di terrorismo o eversione dell’ordine democratico. Accanto alle disposizioni del codice penale, vengono in considerazione i reati previsti in materia da apposite leggi speciali. I reati di terrorismo previsti in leggi speciali attinenti alle più varie materie (ad es. in materia di armi, stupefacenti, di tutela ambientale, ecc.) nonché in tutta quella parte della legislazione italiana, emanata negli anni ‘70 e 80, volta a combattere il terrorismo (ad es. in tema di sicurezza della navigazione aerea e marittima, ecc.).

B) Delitti con finalità di terrorismo previsti dalla Convenzione di New York del 1999.

Il richiamo a tale Convenzione operato dall’art. 25-*quater*, comma 4, del Decreto tende chiaramente ad evitare possibili lacune in quanto con essa si intende promuovere la cooperazione internazionale per la repressione delle condotte di raccolta fondi e di finanziamenti in qualunque forma, destinati ad atti di terrorismo in genere o relativi a settori e modalità a maggior rischio, oggetto di trattati internazionali (trasporti aerei e marittimi, rappresentanze diplomatiche, nucleare, ecc.)

* * *

Sezione II - Delitti di criminalità organizzata

L’art. 24-ter del Decreto, inserito dalla L. n. 94/2009, prevede innanzitutto un gruppo di reati inerenti alle varie forme di associazioni criminose, e cioè:

- Associazione per delinquere generica (art. 416 c.p., primi cinque commi);
- Associazione di tipo mafioso, anche straniera e scambio elettorale politico-mafioso (artt. 416-bis e 416-ter);
- Associazione per delinquere finalizzata alla commissione di delitti in tema di schiavitù, di tratta di persone e di immigrazione clandestina (art. 416 c.p., commi 6 e 7);
- Associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. n. 309/1990).

Con riferimento alle fattispecie di associazioni per delinquere sopra considerate, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione ad una associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) dei reati che costituiscono il fine dell'associazione. Ciò significa che la sola cosciente partecipazione ad una associazione criminosa da parte di un esponente o di un dipendente dell'ente potrebbe determinare la responsabilità amministrativa dell'ente stesso, sempre che la partecipazione o il concorso all'associazione risultasse strumentale al perseguimento anche dell'interesse o del vantaggio dell'ente medesimo. È inoltre richiesto che il vincolo associativo si espliciti attraverso un minimo di organizzazione a carattere stabile nel tempo e la condivisione di un programma di realizzazione di una serie indeterminata di delitti. Non basta cioè l'occasionale accordo per la commissione di uno o più delitti determinati. La giurisprudenza ritiene altresì possibile il concorso nel reato di associazione criminosa da parte di colui che, pur non partecipando all'associazione stessa, fornisca un apporto sostanziale, anche se episodico, alla sua sussistenza od al perseguimento dei suoi scopi.

L'associazione di tipo mafioso (art. 416-bis c.p.) si distingue dalla associazione per delinquere generica per il fatto che coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, oppure - anche non mediante la commissione di delitti, ma pur sempre con l'uso del metodo mafioso - per acquisire in modo diretto od indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

La norma si applica anche alla camorra e alle altre associazioni, comunque denominate, anche straniere, che presentino i connotati mafiosi predetti. Lo scambio elettorale politico-mafioso invece è commesso da chi propone o accetta la promessa di procurare voti con l'uso del metodo mafioso in cambio dell'erogazione o della promessa di denaro o di altra utilità.

Gli altri due tipi di associazioni criminali (art. 416, commi 6 e 7, c.p. e art. 74 D.P.R. n. 309/1990) sono invece caratterizzate dall'essere preordinate al fine della commissione degli specifici reati in esse considerati, vale a dire: dei reati in tema di schiavitù, di tratta di persone, di immigrazione clandestina, di traffico di organi, di reati sessuali contro i minori nonché dei reati di illecita produzione, traffico o detenzione di sostanze stupefacenti o psicotrope. Alcuni di questi specifici reati-fine costituiscono di per sé autonomi reati presupposto della responsabilità dell'ente, come meglio si dirà nel prosieguo a proposito dei reati contro la persona e dei reati transnazionali.

L'art. 24-ter prevede inoltre la generica categoria dei delitti di qualsivoglia tipo, commessi avvalendosi del metodo mafioso od al fine di favorire l'attività di una associazione mafiosa, fermo restando, per la responsabilità dell'ente, il requisito dell'interesse o del vantaggio del medesimo.

La prima circostanza si ritiene ricorra allorché il soggetto agente, pur senza appartenere al sodalizio criminoso o concorrere con esso, pone in essere una condotta idonea ad esercitare una particolare intimidazione, quale ad esempio la minaccia avvalendosi dello sfruttamento della “fama” di organizzazioni criminali operanti nell’ambito di un determinato territorio. L’ipotesi della commissione di un reato di qualsiasi tipo atto ad agevolare l’attività di una associazione mafiosa si verifica quando il soggetto abbia agito con tale scopo specifico e la sua condotta sia concretamente idonea a realizzare tale risultato, come ad esempio nel caso del reato di riciclaggio compiuto essendo a conoscenza della riferibilità dell’operazione ad una associazione mafiosa.

Infine, ai sensi del medesimo art. 24-ter, rilevano i seguenti reati, solitamente, anche se non necessariamente, realizzati nell’ambito di organizzazioni criminali.

Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.).

Il reato consiste nel sequestro di una persona con lo scopo di conseguire per sé o per altri un ingiusto profitto in cambio della liberazione. Il profitto potrebbe anche consistere in un vantaggio di natura non patrimoniale. In casi particolari potrebbero essere ritenuti corresponsabili del reato anche coloro che, pur non avendo partecipato al sequestro, si attivino per far sì che gli autori possano conseguire il riscatto, contribuendo al protrarsi delle trattative e conseguentemente, della privazione della libertà personale del sequestrato, o al conseguimento del profitto da parte dei sequestratori. Potrebbe invece integrare il reato di riciclaggio l’attività di chi interviene nel trasferimento, nella circolazione o nell’impiego di somme di denaro o di altri beni, essendo a conoscenza della provenienza dal reato in questione.

Delitti in tema di armi e di esplosivi (art. 407 comma 2, lettera a), n. 5 c.p.p.).

Si tratta di fattispecie previste dalle leggi speciali vigenti in materia (in particolare dalla L. n. 110/1975 e dalla L. n. 895/1967), che puniscono le condotte di illegale fabbricazione, introduzione nello Stato, vendita, cessione, detenzione e porto abusivo di esplosivi, di armi da guerra e di armi comuni da sparo, con esclusione di quelle da bersaglio da sala, o ad emissione di gas, o ad aria compressa. Anche in questo caso, come per il reato precedente, eventuali collusioni in qualsiasi forma degli operatori bancari con gli autori dei reati in questione o l’espletamento di attività, quali ad esempio la concessione di finanziamenti, con la consapevolezza di anche solo indirettamente favorirli, potrebbe comportare il concorso nei reati stessi o l’imputabilità per altri reati, quali ad esempio il riciclaggio.

* * *

Sezione III - Delitti transnazionali

La responsabilità degli Enti per tale categoria di reati è sancita dalla L. n. 146/2006, al fine di più efficacemente contrastare le organizzazioni criminali che agiscono a livello internazionale.

Si considera transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato e:

- sia commesso in più di uno Stato;

- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero sia commesso in uno Stato, ma abbia effetti sostanziali in un altro Stato.

Si descrivono di seguito le fattispecie penali che, se integrate dagli elementi costitutivi dell'interesse o del vantaggio dell'ente e della transnazionalità (sui quali pure si ritiene debba sussistere la consapevolezza da parte del soggetto agente), possono dar luogo alla responsabilità dell'ente.

Associazioni per delinquere previste dagli artt. 416 e 416-bis c.p. ovvero finalizzate al contrabbando di tabacchi lavorati esteri (art. 291-quater D.P.R. n. 43/1973) o al traffico di stupefacenti (art. 74 D.P.R. n. 309/1990)

Per la definizione delle condotte di base dei reati associativi in questione si rimanda a quanto sopra osservato a proposito dei delitti di criminalità organizzata. Si ritiene che, ricorrendo le caratteristiche della transnazionalità, siano applicabili all'ente unicamente le sanzioni previste dalla L. n. 146/2006 e non anche quelle di cui all'art. 24-ter del Decreto.

Reati in tema di immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5 del D. Lgs. n. 286/1998)³⁰

La norma punisce le condotte consistenti nel trasportare illegalmente stranieri nel territorio dello Stato, nel promuovere, dirigere, organizzare o finanziare tale trasporto, oppure in altri atti diretti a procurare illegalmente l'ingresso di stranieri nel territorio italiano o di uno Stato diverso da quello di loro appartenenza o residenza permanente. E' però richiesto che ricorra almeno una delle cinque condizioni elencate dalla norma stessa³¹.

Le medesime condotte sono punite più severamente se si verifichi la contemporanea presenza di almeno due delle cinque condizioni predette oppure se siano commesse con determinate finalità, quali: il reclutamento di persone destinate alla prostituzione; lo sfruttamento sessuale o lavorativo, lo sfruttamento di minori, o in genere, la finalità di trarre un profitto anche indiretto.

Infine, il comma 5 punisce il favoreggiamento della permanenza dello straniero al fine di trarre un ingiusto profitto dalla sua condizione di illegalità. Si deve ritenere che l'ingiusto profitto sussista quando l'equilibrio delle prestazioni sia fortemente alterato, quale conseguenza dello sfruttamento da parte del soggetto agente dello stato di clandestinità, da lui conosciuto.

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)

³⁰ I reati in tema di immigrazioni clandestine, anche se privi delle caratteristiche della transnazionalità, comportano la responsabilità ai sensi del D. Lgs. 231/2001, a decorrere dal 19 novembre 2017, data di entrata in vigore dell'art. 25-duodecies, comma 1-bis, del Decreto, introdotto dalla L. n. 161/2017.

³¹ In sintesi: a) procurato ingresso o permanenza illegale di cinque o più persone; b) pericolo per l'incolumità delle persone trasportate; c) loro trattamento degradante; d) fatti commessi da tre o più persone concorrenti o con utilizzo di servizi di trasporto internazionali o di documenti falsi o illegalmente ottenuti; e) fatti commessi da chi è nella disponibilità di armi o di esplosivi.

Il reato è commesso da chi, con violenza o minaccia o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci coloro che siano chiamati a rendere dichiarazioni davanti all'autorità giudiziaria, utilizzabili in un procedimento penale, ed abbiano la facoltà di non rispondere.

Si precisa che tale reato può dar luogo alla responsabilità dell'ente anche se commesso senza le caratteristiche della transnazionalità, essendo richiamato, oltre che dalla Legge n.146/2006, anche dall'art. 25-decies del Decreto.

Favoreggiamento personale (art. 378 c.p.)

La condotta criminosa consiste nel prestare aiuto a taluno - dopo l'avvenuta commissione di un delitto per il quale la legge stabilisce l'ergastolo o la reclusione e fuori dei casi di concorso nel medesimo - ad eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa. Il reato sussiste anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto. La pena è aggravata quando il delitto commesso è quello di associazione mafiosa.

Si precisa che, per giurisprudenza maggioritaria, integrano il reato anche le false risposte, tese ai fini di cui sopra, alle richieste dell'Autorità Giudiziaria.

* * *

Sezione IV - Delitti contro la persona

L'art. 25-*quinquies* del Decreto elenca talune fattispecie di reato poste a presidio della personalità individuale previste dal codice penale col fine di contrastare aspramente il fenomeno delle "nuove schiavitù" quali prostituzione, tratta degli esseri umani, sfruttamento dei minori, accattonaggio, attività strettamente collegate al proliferare della criminalità organizzata e delle "nuove mafie".

In particolare, sono contemplate le fattispecie delittuose qui di seguito elencate: "**Riduzione o mantenimento in schiavitù**" (art. 600 c.p.), "**Prostituzione minorile**" (art. 600-bis c.p.), "**Pornografia minorile**" (art. 600-ter c.p.), "**Detenzione di materiale pornografico**" (art. 600-*quater* c.p.), "**Iniziativa turistiche volte allo sfruttamento della prostituzione minorile**" (art. 600-*quinquies* c.p.), "**Adescamento di minorenni**" (art. 609-*undecies* c.p.), "**Tratta di persone**" (art. 601 c.p.), "**Acquisto e alienazione e di schiavi**" (art. 602 c.p.).

Infine, si ricorda che l'art. 25-*quater* 1 dispone la punibilità dell'ente nel caso di commissione del reato contro la persona di cui all'art. 583-bis c.p. (Pratiche di mutilazione degli organi genitali femminili).

Il rischio di responsabilità per i delitti in questione si può ritenere rilevante solo con riferimento all'ipotesi in cui un esponente o un dipendente della Sede Secondaria agiscano in concorso con l'autore materiale del reato. La forma di concorso che presenta maggiori profili di rischio potrebbe essere quella connessa alla messa a disposizione di risorse finanziarie o economiche in favore di organizzazioni o di soggetti che pongano in essere reati dei tipi sopra menzionati.

Tra i reati di questa Sezione possono collocarsi anche i delitti di:

- "**Impiego di cittadini di paesi terzi il cui soggiorno è irregolare**" (art. 22, comma 12-bis, del D. Lgs. n. 286/1998 - Testo Unico

- sull'immigrazione, richiamato dall'art. 25-duodecies del Decreto³²), che punisce i datori di lavoro che assumano o si avvalgano di dipendenti extracomunitari privi di permesso di soggiorno, ovvero scaduto senza che sia richiesto il rinnovo, revocato, o annullato. La responsabilità dell'ente per tale reato, attiguo al reato di sfruttamento di lavoratori clandestini, è prevista solo al ricorrere di determinate circostanze aggravanti³³.
- **“Intermediazione illecita e sfruttamento del lavoro”** (art. 603 bis c.p., richiamato dall'art. 25-quinquies del Decreto³⁴), che punisce chi, approfittando dello stato di bisogno dei lavoratori, intermedia, utilizza, assume o impiega manodopera in condizioni di sfruttamento. Tra gli indici di sfruttamento sono considerate situazioni quali la corresponsione di retribuzioni difformi dai contratti collettivi, la reiterata violazione della normativa sull'orario di lavoro e i riposi, la violazione delle norme sulla sicurezza e igiene dei luoghi di lavoro.
 - **“Razzismo e xenofobia”** (art. 604 – bis, comma 3, c.p., richiamato dall'art. 25-terdecies del Decreto), che punisce l'incitazione, l'istigazione o la propaganda della discriminazione o della violenza per motivi razziali, etnici, nazionali o religiosi, che si basino sulla negazione o minimizzazione della Shoah o di altri crimini di genocidio, di guerra o contro l'umanità.

* * *

Sezione V - Reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa

L'art. 25-*quaterdecies* del Decreto richiama i reati di frode in competizioni sportive e di esercizio abusivo di attività di giuoco o di scommessa. In particolare, con il delitto di frode sportiva è punito chiunque al fine di falsare il risultato di una competizione sportiva organizzata dalle federazioni riconosciute offre o promette denaro o altra utilità o vantaggio a taluno dei partecipanti, o compie altri atti fraudolenti al medesimo scopo. Sono inoltre richiamati i delitti e le contravvenzioni in tema di esercizio, organizzazione, vendita di lotterie, di giochi e scommesse e di utilizzo di apparecchi per il gioco d'azzardo in assenza o violazione delle prescritte autorizzazioni o concessioni.

5.3. Attività aziendali sensibili

Il rischio che siano posti in essere i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali, i reati contro la persona e reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa riguarda principalmente, nell'ambito dell'attività finanziaria, le attività di instaurazione dei rapporti con la clientela nell'ambito del servizio di gestione collettiva e di gestione di portafogli, attività che, ai fini della prevenzione dei reati in

³² L'art. 25-duodecies è stato inserito nel D. Lgs. n. 231/2001 dall'art. 2 del D. Lgs. n. 109/2012, in vigore dal 9.8.2012.

³³ Deve sussistere una delle seguenti circostanze: a) impiego di più di tre lavoratori irregolari; b) impiego di lavoratori irregolari minori in età non lavorativa; c) esposizione a situazioni di grave pericolo.

³⁴ Il richiamo dell'art. 603-bis è stato aggiunto all'art. 25-quinquies del Decreto dall'art. 6 della L. n.199/2016, in vigore dal 4.11.2016.

questione, si devono basare sul fondamentale principio dell'adeguata conoscenza della clientela. Tale principio rappresenta uno dei fondamentali requisiti stabiliti dal D. Lgs. n. 231/2007 concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Le attività sopra individuate sono le medesime nelle quali è più alto il rischio che si verifichino anche reati di riciclaggio. Pertanto, ai fini della prevenzione dei reati sopra illustrati, sono ritenuti idonei i principi di controllo e di comportamento individuati nel protocollo inerente al contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose.

Inoltre, per quanto concerne i reati di:

- *“Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria”*, si individua quale attività aziendale sensibile quella inerente alla gestione dei contenziosi e degli accordi transattivi;
- *“Impiego di cittadini di paesi terzi il cui soggiorno è irregolare”*, e *“Intermediazione illecita e sfruttamento del lavoro”*, si individuano quali attività aziendali sensibili per il primo quella inerente alla gestione del processo di selezione e assunzione del personale e per entrambi quella delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali.

Si rimanda pertanto ai protocolli previsti rispettivamente al paragrafo 6, per il *“Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose”*, al paragrafo 3.3.4 per la *“Gestione dei contenziosi e degli accordi transattivi”*, al paragrafo 3.3.6 per la *“Gestione del processo di selezione e assunzione del personale”* e al paragrafo 3.3.5 *“Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali”*.

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.

6. 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

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, 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").

6.2 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 6 - o non presentino le caratteristiche di transnazionalità in precedenza previste³⁵. Da ultimo, l'art. 25-octies è stato modificato aggiungendovi il nuovo reato di autoriciclaggio³⁶.

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

³⁵ Si ricorda che ai sensi dei commi 5 e 6 dell'art. 10 L. n. 146/2006, abrogati dal Decreto antiriciclaggio, il riciclaggio e l'impiego illecito costituivano reati presupposto della responsabilità degli Enti solo se ricorrevano le caratteristiche di transnazionalità previste dall'art. 3 della medesima legge.

³⁶ Il nuovo reato di autoriciclaggio è stato inserito nel codice penale e aggiunto ai reati presupposto del D. Lgs. n. 231/2001 dalla Legge n. 186/2014, entrata in vigore il 1.1.2015.

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 contravenisse 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 conseguire 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 digital”*.

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.³⁷.

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

³⁷ Come precisato dalla Cass. Pen. 4800/2010: In virtù della clausola di riserva dell'art. 648 ter c.p., il rapporto fra il delitto previsto in questa norma e quello dell'art. 648 bis c.p. va definito ricorrendo al criterio della pluralità ovvero della unicità delle azioni, nel senso che se taluno sostituisce il denaro di provenienza illecita con altro denaro e poi impiega il provento derivante da tale opera di ripulitura in attività economiche o finanziarie risponde del reato di cui all'art. 648 bis c.p., mentre costui risponde del reato di cui all'art. 648 ter c.p. se il denaro di provenienza delittuosa viene direttamente impiegato in tali attività e viene così ripulito".

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'autoriciclatore 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.)³⁸.

³⁸ In ordine all'irrelevanza dell'estinzione del reato che costituisce presupposto di un altro reato si veda l'art. 170, comma 1, c.p.; per l'irrelevanza del difetto di una condizione di punibilità o procedibilità si veda l'art. 648, comma 3, c.p., richiamato anche dagli artt. 648-bis, 648-ter e 648-ter.1 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 summenzionati 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.

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*".

6.3 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 (al riguardo si rimanda al paragrafo 5), 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 3.3.4), la Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali (paragrafo 3.3.5) e la Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni (paragrafo 3.3.6 - 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 4.3.1) - 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 regola 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.

6.3.1 Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose

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.

Descrizione del Processo

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 utilizzati³⁹) 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.

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;
- Segregazione dei compiti:

³⁹ ad esempio interposizione di soggetti terzi, impiego di strumenti societari, associativi o fiduciari suscettibili di limitare la trasparenza della proprietà e della gestione; utilizzo di denaro contante o di strumenti al portatore.

- 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*";
 - 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);
- 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 Informativo 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 adottate 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.

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 dichiara 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, di 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. REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

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 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.

7.2 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.)

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 sulla 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.

7.3 Le Attività Aziendali sensibili

La tutela della salute e della sicurezza sul lavoro è materia che pervade ogni ambito ed attività aziendale.

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 salute e

sicurezza sul lavoro. Tale protocollo si completa con la normativa aziendale di dettaglio vigente in argomento.

Detto protocollo si applica anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio dalle altre società del Gruppo e/o *outsourcer* esterni.

7.3.1 Gestione dei rischi in materia di salute e sicurezza sul lavoro anche con riferimento all'attività svolta da appaltatori e subappaltatori

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 adotta e tiene aggiornato il "*Documento di Valutazione dei Rischi*", 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.

Le Strutture aziendali incaricate della gestione della documentazione inerente la 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.

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.

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:

- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi;
- 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 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.

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.
- 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.
- 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 organizzativa⁴⁰, 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;

40 Quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza

- 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 la 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;
- 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..

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;
- 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;
- 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;
- 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.

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.

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.

8. REATI DI CRIMINALITÀ INFORMATICA

8.1. 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* e 25-*novies* 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.

8.2. Le fattispecie di reati previste dagli artt. 24-*bis* e 25-*novies* 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.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

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.

Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall'installazione non autorizzata di un software da parte di un dipendente.

L'art. 617-quinquies punisce il solo fatto della installazione, fuori dai casi consentiti dalla legge, di apparecchiature atte a intercettare, impedire o interrompere le comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)

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.)

**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.

E' 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 ostacolano 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..

Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)

L'art. 615-quater punisce chiunque al fine di procurare a sé od ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde o comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema protetto da misure di sicurezza o comunque fornisce indicazioni idonee al predetto scopo.

L'art. 615-quinquies punisce chiunque si procura, produce, riproduce importa, diffonde, comunica o consegna o mette a disposizione di altri apparecchiature, dispositivi o programmi allo scopo di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione del suo funzionamento.

Tali fattispecie perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (*virus*, *spyware*) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in parola possono risultare propedeutiche.

La prima fattispecie richiede che il reo agisca a scopo di lucro o di altrui danno. Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e mail, etc., da parte di chi, pur non essendo mosso da specifica finalità di lucro o di causazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

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 civilistiche⁴¹.

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.).

41 Si rammenta al riguardo che, ai sensi del Codice dell'amministrazione digitale (cfr. art. 1, lettera p) del D. Lgs.

n. 82/2005), il documento informatico è "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", ma:

- se non è sottoscritto con una firma elettronica (art. 1, lettera q), non può avere alcuna efficacia probatoria, ma può al limite, a discrezione del Giudice, soddisfare il requisito legale della forma scritta (art. 20, c. 1 bis);
- anche quando sia firmato con una firma elettronica "semplice" (cioè non qualificata) può non avere efficacia probatoria (il giudice dovrà infatti tener conto, per attribuire tale efficacia, delle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità del documento informatico);
- il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata ha l'efficacia prevista dall'articolo 2702 del codice civile (al pari della scrittura privata), fa cioè piena prova, fino a querela di falso, se colui contro il quale è prodotto ne riconosce la sottoscrizione

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 qualificato⁴². 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)⁴³

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

⁴² Per certificato qualificato si intende, ai sensi dell'art. 1 lettere e) ed f) del D. Lgs. n. 82/2005, l'attestato elettronico che collega all'identità del titolare i dati utilizzati per verificare le firme elettroniche, che sia conforme ai requisiti stabiliti dall'allegato I della direttiva 1999/93/CE, rilasciato da certificatori - vale a dire i soggetti che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi con quest'ultime - che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

⁴³ Per l'attuazione del D.L. n. 105/2019, convertito dalla legge n.133/2019, devono essere emanate disposizioni di attuazione per la definizione dei criteri necessari ad individuare, tra l'altro, gli operatori privati inclusi nel perimetro di sicurezza nazionale cibernetica, tra cui rientrerà la Capogruppo, tenuti al rispetto degli obblighi in questione e le modalità per il loro adempimento.

- 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; al riguardo si rimanda al paragrafo 3.3.1.

8.3. 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.

L'attività sensibile identificata dal Modello nella quale è maggiore il rischio che siano posti in essere i comportamenti illeciti come sopra descritti è la:

- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale⁴⁴.

Si riporta di seguito il protocollo che detta i principi di controllo ed i principi di comportamento applicabili a detta attività e che si completa con la

⁴⁴ Il Patrimonio Informativo aziendale è determinato dall'insieme di dati ed informazioni trattate dalla Società, a prescindere dalla forma con cui sono elaborate, gestite o archiviate.

normativa aziendale di dettaglio che regola l'attività medesima. Detto protocollo si applica anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalle altre società del Gruppo e/o *outsourcer* esterni.

8.3.1. Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale

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 protette⁴⁵.

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.

Descrizione del Processo

⁴⁵ Per la descrizione delle relative condotte si veda il paragrafo 9.

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 altresì hardware e software 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.

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:
 - analisi del rischio IT e definizione dei requisiti di sicurezza informatica;
 - gestione Accessi Risorse Informatiche e Servizi di Sicurezza ICT;
 - gestione normativa e architettura di sicurezza informatica;
 - monitoraggio eventi sicurezza informatica e gestione eventi critici di sicurezza informatica;
 - sicurezza delle terze parti (classificazione e monitoraggio dei fornitori della Sede Secondaria e della Capogruppo);
 - diffusione della cultura di sicurezza informatica;
 - progettazione e realizzazione soluzioni di sicurezza informatica.
- Il processo di prevenzione frodi si articola nelle seguenti fasi:
 - identificazione delle misure atte al rafforzamento della prevenzione;
 - monitoraggio dell'evoluzione delle frodi informatiche e fisiche anche per quanto riguarda eventuali aspetti di sicurezza fisica correlati;
 - presidio delle attività necessarie all'intercettazione e alla soluzione delle minacce verso gli asset aziendali;
 - gestione delle comunicazioni con le Forze dell'Ordine.
- Il processo di gestione della sicurezza fisica si articola nelle seguenti fasi:
 - gestione protezione di aree e locali ove si svolge l'attività;
 - gestione sicurezza fisica dei sistemi periferici (sede centrale, altre sedi).
 - Il processo relativo al servizio di certificazione di firma elettronica si articola nelle seguenti fasi:
 - apertura del contratto;
 - registrazione del titolare;

- gestione del certificato (sospensione, riattivazione, revoca, rinnovo e sblocco PIN).
- 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.

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 deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica dei processi sopra descritti. In particolare:
 - la gestione delle abilitazioni avviene tramite la definizione di "profili di accesso" in ragione delle funzioni svolte all'interno della Sede Secondaria;
 - le variazioni al contenuto dei profili sono eseguite dalle Strutture della Sede Secondaria deputate al presidio della sicurezza logica, su richiesta delle Strutture interessate. La Struttura richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative coperte;
 - ogni utente ha associato un solo profilo abilitativo in relazione al proprio ruolo aziendale nel rispetto del principio del minimo privilegio. In caso di trasferimento o di modifica dell'attività dell'utente, viene attribuito il profilo abilitativo corrispondente al nuovo ruolo assegnato.
- Segregazione dei compiti:
 - sono assegnati distinti ruoli e responsabilità di gestione della sicurezza delle informazioni; in particolare:
 - sono attribuite precise responsabilità in modo che siano presidiati gli ambiti di indirizzo e governo della sicurezza, di progettazione, di implementazione, di

- esercizio e di controllo delle contromisure adottate per la tutela del Patrimonio Informativo aziendale;
- sono attribuite precise responsabilità per la gestione degli aspetti di sicurezza alle funzioni organizzative che sviluppano e gestiscono sistemi informativi;
 - sono definite le responsabilità ed i meccanismi atti a garantire la gestione di eventi di sicurezza anomali, delle situazioni di emergenza e crisi e delle relative comunicazioni alle Autorità Preposte;
 - sono attribuite precise responsabilità della predisposizione, validazione, emanazione e aggiornamento delle norme di sicurezza a funzioni aziendali distinte da quelle incaricate della gestione;
 - le attività di implementazione e modifica dei software, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del software sono organizzativamente demandate a strutture differenti rispetto agli utenti, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi;
 - sono attribuite precise responsabilità per garantire che il processo di sviluppo e manutenzione delle applicazioni, effettuato internamente o presso terzi, sia gestito in modo controllato e verificabile attraverso un opportuno iter autorizzativo.
- Attività di controllo: le attività di gestione ed utilizzo dei sistemi informativi della Sede Secondaria e del Patrimonio Informativo aziendale sono soggette ad una costante attività di controllo che si esplica sia attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità con particolare riferimento al trattamento dei dati personali, sia tramite l'adozione, per l'insieme dei processi aziendali, di specifiche soluzioni di continuità operativa di tipo tecnologico, organizzativo e infrastrutturale che assicurino la predetta continuità anche a fronte di situazioni di emergenza. Le attività di controllo costituiscono valido presidio anche a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate.

I controlli previsti, declinati dalle relative policy interne, si basano sulla definizione di specifiche attività finalizzate alla gestione nel tempo anche degli aspetti inerenti alla protezione del Patrimonio Informativo del Gruppo, quali:

- la definizione degli obiettivi e delle strategie di sicurezza;
- la definizione di una metodologia di analisi dei rischi ai quali è soggetto il patrimonio informativo da applicare a processi ed asset aziendali, stimando la criticità delle informazioni in relazione ai criteri di riservatezza, integrità e disponibilità;
- l'individuazione delle contromisure adeguate, con riferimento ai livelli

di rischio rilevati, verificando e controllando il corretto mantenimento dei livelli di sicurezza stabiliti;

- l'adeguata formazione del personale sugli aspetti di sicurezza per sviluppare una maggiore sensibilità;
- la predisposizione e l'aggiornamento delle norme di sicurezza, al fine di garantirne nel tempo l'applicabilità, l'adeguatezza e l'efficacia;
- i controlli sulla corretta applicazione ed il rispetto della normativa definita.
- Le principali attività di controllo, tempo per tempo effettuate, e specificamente dettagliate nella normativa interna di riferimento, sono le seguenti:
 - Con riferimento alla sicurezza fisica:
 - protezione e controllo delle aree fisiche (perimetri/zone riservate) in modo da scongiurare accessi non autorizzati, alterazione o sottrazione degli asset informativi.
 - Con riferimento alla sicurezza logica:
 - identificazione e autenticazione dei codici identificativi degli utenti;
 - autorizzazione relativa agli accessi alle informazioni richiesti;
 - previsione di tecniche crittografiche e di firma digitale per garantire la riservatezza, l'integrità e il non ripudio delle informazioni archiviate o trasmesse.
 - Con riferimento all'esercizio ed alla gestione di applicazioni, sistemi e reti:
 - previsione di una separazione degli ambienti (sviluppo, collaudo e produzione) nei quali i sistemi e le applicazioni sono installati, gestiti e mantenuti in modo tale da garantire nel tempo la loro integrità e disponibilità;
 - predisposizione e protezione della documentazione di sistema relativa alle configurazioni, personalizzazioni e procedure operative, funzionale ad un corretto e sicuro svolgimento delle attività;
 - previsione di misure per le applicazioni in produzione in termini di installazione, gestione dell'esercizio e delle emergenze, protezione del codice, che assicurino il mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni trattate;
 - attuazione di interventi di rimozione di sistemi, applicazioni e reti individuati come obsoleti;
 - pianificazione e gestione dei salvataggi di sistemi operativi, software, dati e delle configurazioni di sistema;
 - gestione delle apparecchiature e dei supporti di memorizzazione per garantire nel tempo la loro integrità e disponibilità tramite la regolamentazione ed

- il controllo sull'utilizzo degli strumenti, delle apparecchiature e di ogni asset informativo in dotazione nonché mediante la definizione di modalità di custodia, riutilizzo, riproduzione, distruzione e trasporto fisico dei supporti rimovibili di memorizzazione delle informazioni, al fine di proteggerli da danneggiamenti, furti o accessi non autorizzati;
- monitoraggio di applicazioni e sistemi, tramite la definizione di efficaci criteri di raccolta e di analisi dei dati relativi, al fine di consentire l'individuazione e la prevenzione di azioni non conformi;
 - prevenzione da software dannoso tramite sia opportuni strumenti ed infrastrutture adeguate (tra cui i sistemi antivirus) sia l'individuazione di responsabilità e procedure per le fasi di installazione, verifica di nuovi rilasci, aggiornamenti e modalità di intervento nel caso si riscontrasse la presenza di software potenzialmente dannoso;
 - formalizzazione di responsabilità, processi, strumenti e modalità per lo scambio delle informazioni tramite posta elettronica e siti web;
 - adozione di opportune contromisure per rendere sicura la rete di telecomunicazione e gli apparati a supporto e garantire la corretta e sicura circolazione delle informazioni;
 - previsione di specifiche procedure per le fasi di progettazione, sviluppo e cambiamento dei sistemi e delle reti, definendo i criteri di accettazione delle soluzioni;
 - previsione di specifiche procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge e contrattuali;
- Con riferimento allo sviluppo ed alla manutenzione delle applicazioni:
- individuazione di opportune contromisure ed adeguati controlli per la protezione delle informazioni gestite dalle applicazioni, che soddisfino i requisiti di riservatezza, integrità e disponibilità delle informazioni trattate, in funzione degli ambiti e delle modalità di utilizzo, dell'integrazione con i sistemi esistenti e del rispetto delle disposizioni di Legge e della normativa interna;
 - previsione di adeguati controlli di sicurezza nel processo di sviluppo delle applicazioni, al fine di garantirne il corretto funzionamento anche con riferimento agli accessi alle sole persone autorizzate,

- mediante strumenti, esterni all'applicazione, per l'identificazione, l'autenticazione e l'autorizzazione.
- Con riferimento alla gestione degli incidenti di sicurezza:
 - previsione di opportuni canali e modalità di comunicazione per la tempestiva segnalazione di incidenti e situazioni sospette al fine di minimizzare il danno generato e prevenire il ripetersi di comportamenti inadeguati e attivare l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi.
 - Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;
 - tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente, ecc.), con particolare riguardo all'operato di utenze con privilegi speciali, risultano tracciate attraverso sistematica registrazione (sistema di log files);
 - tutti i transiti in ingresso e in uscita degli accessi alle zone riservate, del solo personale che ne abbia effettiva necessità previa debita autorizzazione, sono rilevati tramite appositi meccanismi di tracciatura;
 - è prevista la tracciatura delle attività effettuate sui dati, compatibili con le leggi vigenti 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.

Principi di comportamento

Le Strutture 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.

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, trojan, 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 costituente;
 - 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.

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

9.1 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.

9.2 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 commercio⁴⁶, mentre l'art. 25-novies - al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno⁴⁷ 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. **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 falsificazione⁴⁸.

Integrano la contraffazione le ipotesi consistenti nella riproduzione identica

⁴⁶ A seguito della modifica apportata dalla L. n. 99/2009, l'art. 25-bis del D. Lgs. n. 231/2001 - che in precedenza riguardava i soli ai reati di falsità in materia di monete e di valori di bollo - concerne anche i delitti previsti dagli articoli 473 e 474 c.p., i quali hanno in comune con i primi il bene giuridico principalmente tutelato e cioè la fede pubblica, intesa quale affidamento che la generalità dei cittadini ripone nella veridicità di determinati oggetti, segni o attestazioni.

⁴⁷ Ai sensi dell'art. 1 della L. n. 633/1941 sono tutelate le opere dell'ingegno di carattere creativo che appartengono alla letteratura (anche scientifica o didattica), alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì protetti come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

⁴⁸ Per “fare uso” dei marchi falsi dovrebbero intendersi condotte residuali, quali ad esempio l'apposizione su propri prodotti di marchi falsificati da terzi. Si deve trattare cioè di condotte diverse sia dalla messa in circolazione di prodotti recanti marchi falsi previste nell'art. 474 c.p., sia dalle condotte più propriamente realizzative della contraffazione, quale ad esempio la riproduzione del marchio altrui nelle comunicazioni pubblicitarie, nella corrispondenza commerciale, nei siti internet, ecc..

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. E' 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 altrui⁴⁹. 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. E' 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.

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

⁴⁹ Il Codice della proprietà industriale (D. Lgs. n. 30/2005), all'art. 2 recita: "La brevettazione e la registrazione danno luogo ai titoli di proprietà industriale. Sono oggetto di brevettazione le invenzioni, i modelli di utilità, le nuove varietà vegetali. Sono oggetto di registrazione i marchi, i disegni e modelli, le topografie dei prodotti a semiconduttori."

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 distintivi⁵⁰ atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto. E' 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).

⁵⁰ L'art. 181-bis, comma 8, della L. n. 633/1941 dispone che ai fini della legge penale il contrassegno SIAE è considerato segno distintivo di opera dell'ingegno.

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'origine⁵¹ 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 altrui⁵².

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.

⁵¹ Ai sensi dell'art. 29 del D. Lgs. n. 30/2005 sono protette: "le indicazioni geografiche e le denominazioni di origine che identificano un paese, una regione o una località, quando siano adottate per designare un prodotto che ne è originario e le cui qualità, reputazione o caratteristiche sono dovute esclusivamente o essenzialmente all'ambiente geografico d'origine, comprensivo dei fattori naturali, umani e di tradizione".

⁵² Si veda ad es. l'art. 65 della L. n. 633/1941, secondo il quale gli articoli di attualità pubblicati nelle riviste e nei giornali possono essere utilizzati da terzi, se la riproduzione non è stata espressamente riservata, purché si indichino la fonte, la data e l'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 elaboratore⁵³, 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 dati⁵⁴, 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 costituente⁵⁵ 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 trarre 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)

⁵³ Ai sensi dell'art. 2, n. 8, della L. n. 633/1941 sono tutelati i programmi per elaboratore in qualsiasi forma espressi purché originali, quale risultato di creazione intellettuale dell'autore. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso. Gli artt. 64-bis, 64-ter e 64-quater della citata legge disciplinano l'estensione dei diritti che competono all'autore del programma e i casi di libera utilizzazione dello stesso, vale a dire le ipotesi in cui sono consentite riproduzioni od interventi sul programma anche senza specifica autorizzazione del titolare dei diritti.

⁵⁴ Ai sensi dell'art. 2, n. 9, della L. n. 633/1941, le banche di dati consistono in raccolte di opere, dati od altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici od in altro modo. Resta ovviamente salva la distinta tutela riconosciuta ai diritti d'autore eventualmente esistenti sulle opere dell'ingegno inserite nella banca dati. Gli artt. 64-quinquies e 64-sexies della legge disciplinano l'estensione dei diritti dell'autore della banca di dati nonché i casi di libera utilizzazione della stessa.

⁵⁵ I diritti del costituente sono regolati dagli artt. 102-bis e 102-ter della L. n. 633/1941. Per costituente si intende colui che effettua investimenti rilevanti per la creazione, la verifica o la presentazione di una banca di dati ed al quale compete, indipendentemente dalla tutela che spetta al suo autore in ordine ai criteri creativi secondo i quali il materiale è stato scelto ed organizzato, il diritto di vietare le operazioni di estrazione o di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati. Per le banche di dati messe a disposizione del pubblico, ad esempio mediante libero accesso on line, gli utenti, anche senza espressa autorizzazione del costituente, possono effettuare estrazioni o reimpieghi di parti non sostanziali, valutate in termini qualitativi e quantitativi, per qualsivoglia fine, salvo che l'estrazione od il reimpiego siano stati espressamente vietati o limitati dal costituente.

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 vogliono avvalersi dell'esenzione dall'obbligo di apposizione del contrassegno SIAE⁵⁶.

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.

⁵⁶ L'art. 181-bis, comma 3, della L. n. 633/1941 dispone che, fermo restando il rispetto dei diritti tutelati dalla legge, possono essere privi del contrassegno SIAE i supporti contenenti software da utilizzarsi esclusivamente tramite elaboratore elettronico, che non contengano opere audiovisive intere non realizzate espressamente per il programma per elaboratore, ovvero riproduzioni di parti eccedenti il 50% di preesistenti opere audiovisive, che diano luogo a concorrenza nell'utilizzazione economica delle stesse.

9.3 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;

- ;
- 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.

Meno rilevante appare il rischio con riferimento alle attività di ideazione e di lancio di nuovi prodotti, di gestione del *namings* e dei marchi del Gruppo, della comunicazione esterna o pubblicitaria e delle iniziative di *marketing*, nonché con riferimento alle attività di gestione dei rapporti con la clientela, nell'ottica della lealtà della concorrenza e della correttezza e trasparenza delle pratiche commerciali, e ciò in ragione della sviluppata articolazione dei presidi di controllo e delle procedure già imposti dalla normativa di settore. Si rimanda pertanto ai protocolli previsti:

- al paragrafo 6 per il "*Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose*";
- al paragrafo 3.3.5 per la "*Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali*";
- al paragrafo 3.3.6 per la "*Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni*";
- al paragrafo 8.3.1 per la "*Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo aziendale*";
- al paragrafo 3.3.1 per la "*Stipula dei rapporti contrattuali con la Pubblica Amministrazione*",

i quali contengono processi, principi di controllo e principi di comportamento diretti a prevenire anche la commissione dei reati di cui al presente Capitolo.

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalle altre sedi del Gruppo e/o da *outsourcer* esterni.

10. REATI TRIBUTARI

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, 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-*quiquiesdecies* 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.

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

La responsabilità degli enti è estesa ad alcuni dei reati in materia di imposte sui redditi e sul valore aggiunto previsti dal D. Lgs. n. 74/2000, che detta la disciplina di portata generale sui reati tributari, riformata per rafforzare la repressione del fenomeno dell'evasione fiscale.

Le nuove fattispecie in materia tributaria sono state inserite nell'articolo 25-*quiquiesdecies* (reati tributari). 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)

Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. n. 74/2000)

Il primo reato è commesso da 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.

Il secondo 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.

10.3 Le Attività Aziendali sensibili

Il rischio di commissione dei reati tributari può presentarsi in ogni attività aziendale. Esso è specificamente presidiato dal protocollo "Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari".

Per quanto riguarda la posizione di contribuente della Società, tale rischio è inoltre presidiato dal protocollo "Gestione dell'informativa periodica".

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:

- 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 e ed al riciclaggio dei proventi di

- attività criminose;
- che contengono principi di controllo e di comportamento da rispettare anche ai fini della prevenzione dei reati fiscali.

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

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.

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.

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 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.

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. 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 disposizioni 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 artificiali, 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.