APP BROKER S.r.l.

Modello di Organizzazione, Gestione e Controllo *ex* Decreto Legislativo dell'8 giugno 2001 n. 231

(Testo deliberato in C.d.A. il 9 marzo 2015, il 14 marzo 2018 e successivamente modificato l'8 marzo 2019 ed il 23 marzo 2020)

INDICE

PARTE GENERALE

Definizioni

- "Allianz" o "Capogruppo": Allianz S.p.A., con sede legale in Trieste, Largo Irneri 1.
- "Attività/ Aree Sensibili": le attività di APP Broker nel cui ambito sussiste il rischio di commissione dei Reati rilevanti ai sensi del D.lgs. 231/2001.
- "CCNL": i Contratti Collettivi Nazionali di Lavoro stipulati da A.N.I.A. e dalle associazioni sindacali maggiormente rappresentative per il personale dipendente non dirigente delle imprese e i dirigenti delle stesse imprese, oltre che al Contratto Integrativo Aziendale per il personale dirigente, attualmente in vigore ed applicati da APP Broker.
- "Codice Etico e di Comportamento": codice comportamentale adottato dal Gruppo e pubblicato sul sito internet, contenente gli standard minimi che tutti i Destinatari sono tenuti a rispettare al fine di prevenire situazioni che potrebbero minare l'integrità del Gruppo.
- "Consulenti": i soggetti che agiscono in nome e/o per conto della Società in forza di un contratto di mandato o di altro rapporto contrattuale di collaborazione.
- "Datore di Lavoro": il soggetto titolare del rapporto di lavoro o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa in quanto titolare dei poteri decisionali e di spesa.
- "D.lgs. 231/2001" o il "Decreto": il Decreto Legislativo 8 giugno 2001 n. 231 (*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*) e successive modifiche e integrazioni.
- "Decreto Sicurezza": Decreto Legislativo del 9 aprile 2008 n.81 concernente l'attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro.
- "Destinatari": ai sensi dell'art. 5 del D.lgs. n. 231/2001, tutti coloro che rivestono, nella Società, funzioni di rappresentanza, amministrazione e direzione ovvero gestione e controllo (anche di fatto) ed i dipendenti. Il Modello si applica altresì, nei limiti del rapporto in essere, a coloro i quali, pur non appartenendo alla Società, operano su mandato o per conto della stessa o sono comunque ad essa legati da rapporti giuridici rilevanti in funzione della prevenzione dei Reati (collaboratori, consulenti o altri terzi vincolati da un rapporto contrattuale diverso dal lavoro subordinato).

- "Dipendenti": i soggetti in distacco da Allianz S.p.A.(ed aventi con la stessa un rapporto di lavoro subordinato) che prestano servizio per APP Broker, ivi compresi i dirigenti.
- "Gruppo Allianz": ALLIANZ S.p.A. e le società di diritto italiano controllate da ALLIANZ S.p.A. ai sensi dell'art. 2359, primo e secondo comma, del Codice Civile.
- "APP Broker" o "Società".
- "Linee Guida": raccomandazioni delle associazioni di categoria sviluppate sistematicamente sulla base di conoscenze continuamente aggiornate e valide, ad es. le Linee Guida A.N.I.A. e Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo per il settore assicurativo ex articolo 6, comma 3, del D.lgs. 231/2001.
- "Modello" o "MOG": il modello di organizzazione, gestione e controllo previsti dal D.Lgs. 231/2001.
- "Organi Sociali": sia il Consiglio di Amministrazione di APP Broker sia i suoi membri.
- "Operazioni Sensibili": vedi "Attività/ Aree Sensibili".
- "Organismo di Vigilanza" o "OdV": l'organismo interno di controllo, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello nonché al relativo aggiornamento, ai sensi dell'art. 6 del D.Lgs. 231/2001.
- "Pubblica Amministrazione" o "Ente pubblico": a titolo esemplificativo, enti pubblici territoriali e non territoriali (Stato, Regione, Provincia, Comune, Camera di Commercio, ASL, Ispettorato del Lavoro, etc.); enti istituiti e regolamentati con legge dello stato; società con partecipazione pubblica totalitaria o prevalente; società controllate da società con partecipazione pubblica totalitaria o prevalente; concessionari di pubblico servizio.
- "Società di Service": Arpa S.r.l. ed in generale altre eventuali società di service esterne alla Società, nonché le Società del Gruppo Allianz (i.e. Allianz Technology S.c.p.A. ed Allianz S.p.A.) che svolgono attività di servizio in favore di altre società del Gruppo stesso.
- "Soggetti Apicali": 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 persone che esercitano, anche di fatto, la gestione e il controllo dello stesso.
- "SSL": Salute e Sicurezza dei Lavoratori.
- "UIF": Unità di Informazione Finanziaria, intesa come la struttura nazionale – istituita presso la Banca d'Italia dal D.Lgs. n. 231/2007 – incaricata di ricevere dai soggetti obbligati, di richiedere

ai medesimi, di analizzare e di comunicare alle autorità competenti le informazioni che riguardano ipotesi di riciclaggio o di finanziamento del terrorismo.

CAPITOLO 1 – IL DECRETO LEGISLATIVO N. 231/2001

1.1. Il Decreto Legislativo n. 231/2001 e la normativa di riferimento

In data 4 luglio 2001 è entrato in vigore il Decreto Legislativo 231 dell'8 giugno 2001, emanato in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 nonché pubblicato nella Gazzetta Ufficiale del 19 giugno 2001 n. 140, al fine di adeguare la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali, cui l'Italia ha aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione del 26 maggio 1997, anch'essa firmata a Bruxelles, sulla lotta alla corruzione in cui sono coinvolti funzionari della Comunità Europea e degli Stati Membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.
Il Decreto Legislativo 231/2001 reca le disposizioni normative concernenti la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica".

Esaminando nel dettaglio il contenuto del Decreto Legislativo 231/2001, l'articolo 5, 1° comma, sancisce la responsabilità della società qualora determinati reati siano stati commessi nel suo interesse o a suo vantaggio da:

a) 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 persone che esercitano, anche di fatto, la gestione e il controllo della stessa (ad esempio, amministratori e direttori generali);
b) persone sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati alla precedente lettera a) (ad esempio, dipendenti non dirigenti).

Pertanto, nel caso in cui venga commesso uno dei reati specificamente indicati, alla responsabilità penale della persona fisica che ha realizzato materialmente il fatto si aggiunge - se ed in quanto siano integrati tutti gli altri presupposti normativi - anche la responsabilità "amministrativa" della società.
Sotto il profilo sanzionatorio, per tutti gli illeciti commessi è sempre prevista a carico della persona giuridica l'applicazione di una sanzione pecuniaria; per le ipotesi di maggiore gravità è prevista anche

l'applicazione di sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, licenze o concessioni, il divieto di contrarre con la P.A., l'esclusione da finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni e servizi.

Quanto ai reati cui si applica la disciplina in esame, si elencano di seguito le "famiglie di reato" attualmente rientranti nell'ambito di applicazione del D.lgs. 231/2001, rimandando all'**Appendice 1** del presente documento per il dettaglio delle singole fattispecie ricomprese in ciascuna famiglia:

(i) Reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto) e contro la fede pubblica;

(ii) Delitti informatici e trattamento illecito di dati, introdotti dalla Legge 48/2008 (art. 24-bis del Decreto);

(iii) Delitti di criminalità organizzata**,** introdotti dalla Legge 94/2009 (art. 24 ter del Decreto);

(iv) Reati transnazionali**,** introdotti dalla Legge 146/2006;

(v) Reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, introdotti dalla Legge 409/2001 e modificati con Legge 99/2009 (art. 25-bis del Decreto);

(vi) Delitti contro l'industria e il commercio, introdotti dalla Legge 99/2009 (art. 25-bis 1 del Decreto);

(vii) Reati societari**,** introdotti dal D.lgs. 61/2002 e modificati dalla Legge 262/2005 (art. 25-ter del Decreto), anche con specifico riferimento al reato di corruzione tra privati e istigazione alla corruzione tra privati (art. 2635 e 2635 bis c.c.), come introdotto dalla Legge 6 novembre 2012, n. 190;

(viii) Delitti in materia di terrorismo o di eversione dell'ordine democratico, introdotti dalla Legge 7/2003 (art. 25-quater del Decreto);

(ix) Pratiche di mutilazione degli organi genitali femminili, introdotti dalla Legge 7/2006 (art. 25–quater. 1 del Decreto);

(x) Delitti contro la personalità individuale, introdotti dalla Legge 228/2003 e modificati con la Legge 38/2006 (art. 25-quinquies del Decreto);

(xi) Reati ed illeciti amministrativi di Abuso di mercato, introdotti dalla Legge 62/2005 e modificati dalla Legge 262/2005 (art. 25-sexies del Decreto);

(xii) Reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro (omicidio colposo e lesioni gravi o gravissime), introdotti dalla Legge 123/2007 (art. 25-septies del Decreto);

(xiii) Reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio, introdotti dal D.lgs. 231/2007 (art. 25-octies del Decreto);

(xiv) Delitti in materia di violazione del diritto d'autore, introdotti dalla Legge 99/2009 (art. 25-novies del Decreto);

(xv) Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, introdotto dalla Legge 116/2009 (art. 25-decies del Decreto);

(xvi) Reati ambientali, introdotti dal D.lgs. 121/2011 (art. 25-undecies del Decreto);

(xvii) Reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, introdotto dal D.lgs. 109/2012 (art. 25-duodecies del Decreto);

(xviii) Reati di razzismo e xenofobia;

(xix) Frodi in competizioni sportive sportivee i reati di esercizio abusivo di gioco o di scommesse e di giochi d'azzardo esercitati a mezzo di apparecchi vietati

Si tralasciano i reati contro la fede pubblica, i delitti contro la personalità individuale, previsti rispettivamente dagli artt. 25-bis, 25-quinquies (ad esclusione, per ciò che si dirà, della fattispecie di «Intermediazione illecita e sfruttamento del lavoro» ai sensi dell'art. 603-bis c.p.), i reati di razzismo e xenofobia e le frodi sportive, previsti dagli artt. 25-terdecies e 25-quaterdecies del Decreto,che, a seguito di un'analisi delle attività a rischio, sono stati giudicati solo astrattamente ipotizzabili in APP BROKER S.r.l..

1.2. Presupposti di esclusione della responsabilità dell'ente

Il D.Lgs. 231/2001 prevede, all'articolo 6, una forma di esonero dalla responsabilità, in caso di reato compiuto da "soggetti apicali", qualora la società dimostri di aver adottato ed efficacemente attuato "modelli di organizzazione, gestione e controllo" idonei a prevenire la realizzazione degli illeciti penali considerati.

I suddetti Modelli devono rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi i Reati;
- prevedere specifici protocolli (i.e. procedure) diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai Reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei Reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli;
- introdurre un sistema disciplinare privato idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

1. L'art. 6 del D.Lgs. 231/2001 prevede inoltre che l'ente, ai fini dell'esclusione della responsabilità per il reato commesso da soggetto "apicale", debba provare che: l'ente abbia provveduto all'istituzione di un organo di controllo interno all'ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei Modelli nonché di curarne l'aggiornamento;
2. l'organismo di controllo non sia colpevole di omessa o insufficiente vigilanza in merito all'attuazione e all'osservanza del Modello;
3. l'ente abbia predisposto un sistema di verifica periodica e di eventuale aggiornamento del Modello;
4. l'autore del reato abbia agito eludendo fraudolentemente le disposizioni del Modello.

Accanto a tali previsioni, la Legge 30 novembre 2017, n. 179 recante «Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato» ha aggiunto nel corpo del Decreto una serie di ulteriori prescrizioni (nello specifico, art. 6, commi 2-bis, 2-ter e 2-quater), volti a garantire tutela e protezione a quanti, all'interno dell'ente, segnalino tempestivamente la commissione di condotte illecite rilevanti ai sensi del Decreto (c.d. whistleblowing).

In particolare, ai sensi dell'art. 6, comma 2-bis, lett. a), il Modello deve ora anche prevedere uno o più canali che consentano tanto ai soggetti apicali, tanto ai soggetti subordinati, «di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del […] decreto

e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte». Tali canali di comunicazione devono anche garantire «la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione».

Inoltre, il medesimo comma 2-bis precisa inoltre (lett. b) che il Modello deve poi individuare almeno un canale alternativo di segnalazione «idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante». Ancora, sempre il nuovo comma 2-bis sancisce (lett. c) ora il divieto di atti di ritorsione o comunque discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. Infine, si stabilisce anche (lett. d) che il Modello debba individuare nel sistema disciplinare adottato ai sensi del Decreto sanzioni «nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate».

Ai sensi dell'art. 7 del D.Lgs. 231/2001, la responsabilità amministrativa dell'ente per il reato compiuto da "soggetti sottoposti all'altrui direzione" sussiste se la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza (cd. colpa di organizzazione). L'efficace attuazione di un Modello idoneo a prevenire la realizzazione degli illeciti penali considerati costituisce prova dell'assenza di colpa di organizzazione e preclude l'insorgenza di una responsabilità dell'ente. Lo stesso D.lgs. 231/2001, nonché il relativo Regolamento di attuazione emanato con Decreto Ministeriale del 26 giugno 2003 n. 201, afferma inoltre che i Modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni osservazioni sulla idoneità dei Modelli a prevenire i Reati.

CAPITOLO 2 – LINEE GUIDA A.N.I.A

2.1 Linee Guida di riferimento

Nella predisposizione del presente Modello, APP Broker si è ispirata alle Linee Guida A.N.I.A.[1], essendo intermediario assicurativo, nonché parte di un Gruppo Assicurativo, salvo che per i necessari adattamenti dovuti alla particolare struttura organizzativa aziendale del Gruppo ALLIANZ.

Qui di seguito si riportano in sintesi gli elementi di maggior rilevanza.

I punti fondamentali che le Linee Guida individuano nella costruzione dei Modelli possono essere così sintetizzati e schematizzati:

- individuazione delle aree/attività di rischio, volta a verificare in quale area/attività aziendale sia possibile la realizzazione dei Reati suscettibili di dare luogo ad una responsabilità dell'ente ai sensi del Decreto;
- obblighi di informazione dell'organismo di vigilanza, volti a soddisfare l'attività di controllo sul funzionamento, l'efficacia e l'osservanza del Modello;
- predisposizione di un sistema di controllo interno ragionevolmente in grado di prevenire o ridurre il rischio di commissione dei Reati attraverso l'adozione di appositi protocolli. A tal fine soccorre l'insieme ben coordinato di strutture organizzative, attività e regole attuate – su impulso dell'organo decisionale – dal *management* e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti nelle seguenti categorie:
  - efficacia ed efficienza dei processi aziendali e delle operazioni gestionali;
  - adeguato controllo dei rischi;
  - attendibilità ed integrità delle informazioni aziendali – contabili e gestionali – dirette sia verso terzi sia all'interno;
  - salvaguardia del patrimonio;
  - conformità dell'attività dell'impresa alla normativa vigente e alle direttive e procedure aziendali.

[1] Linee Guida per il settore assicurativo in materia di responsabilità amministrativa (ex art.6 comma 3 del D.Lgs. 8.6.2001 n.231), aggiornate al 18 marzo 2008.

In particolare, le componenti più rilevanti del sistema di controllo interno possono essere indicate nei seguenti strumenti:

- Codice Etico e di Comportamento;
- sistema organizzativo, procedure manuali ed informatiche;
- poteri autorizzativi e di firma;
- sistemi di controllo e di gestione;
- comunicazioni al personale;
- formazione del personale;
- meccanismi disciplinari.

Le componenti del sistema di controllo interno devono pertanto essere informate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- applicazione di regole e criteri improntate a principi di trasparenza;
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle regole e delle procedure previste dal Modello;
- individuazione dei requisiti dell'organismo di vigilanza, riassumibili come segue:
  - autonomia ed indipendenza;
  - professionalità;
  - continuità di azione;
  - assenza di cause di incompatibilità, di conflitti di interesse o rapporti di parentela con gli organi di vertice.

In quest'ottica, è ipotizzabile adottare soluzioni organizzative che accentrino presso la Capogruppo le funzioni previste dal D.lgs. 231/2001, a condizione che:

- in omaggio ai principi di autonomia e di responsabilità proprie di ciascuna società, ogni controllata adotti un proprio modello di organizzazione, gestione e controllo ex Decreto, ispirato – per quanto possibile – alle linee guida della Capogruppo;
- in ogni controllata sia istituito il proprio organismo di vigilanza ovvero, allorquando per motivi di concentrazione e ottimizzazione dell'efficienza dei controlli l'organismo di vigilanza sia unico per tutte o alcune delle imprese del gruppo, ognuna delle società controllate assegni ufficialmente a detto organo l'incarico di vigilanza sul proprio modello risultando quindi disporre di un proprio organismo di vigilanza;
- i rapporti di assistenza e collaborazione tra l'organismo di vigilanza della Capogruppo e quelli propri delle singole società controllate siano definiti con appositi strumenti contrattuali;
- nell'esecuzione delle attività di assistenza e collaborazione tra gli organismi di vigilanza della Capogruppo e delle singole controllate, siano assicurati il rispetto degli obblighi di fedeltà e riservatezza nei confronti dell'organismo di vigilanza richiedente.

CAPITOLO 3 – IL MODELLO DI APP BROKER

3.1. Le principali aree di operatività aziendale e la struttura organizzativa di APP BROKER

APP Broker è una società appartenente al Gruppo ALLIANZ, controllata e soggetta all'attività di direzione e coordinamento da parte di ALLIANZ S.p.A., società che opera nel settore assicurativo.

La Società ha per oggetto l'attività di mediazione assicurativa e riassicurativa, limitatamente al ramo danni. In particolare l'attività di APP Broker consiste nel promuovere prodotti assicurativi di Compagnie specializzate o Compagnie internazionali che non hanno reti distributive in Italia, con le quali APP Broker ha in essere un accordo di collaborazione/distribuzione dei relativi prodotti.

La Società svolge le proprie attività di brokeraggio presso altre agenzie assicurative (in particolare del Gruppo Allianz) o broker, con i quali stipula specifici mandati di collaborazione.

La struttura organizzativa/operativa di APP Broker risulta composta da:

- Consiglio di Amministrazione;
- Responsabile operativo di APP Broker, nonché membro del Consiglio di Amministrazione (nella persona del Responsabile dell'Unità Organizzativa Mid Corporate e Riassicurazione di Allianz S.p.A.);
- Personale in distacco da Allianz S.p.A., a cui sono affidate le seguenti attività:
    - gestione dei rapporti con la rete, sviluppo e gestione della rete (i.e. interfaccia con Agenti e Broker);
    - supporto per tematiche relative all'assunzione del rischio, alle caratteristiche e all'emissione di prodotti collocati dalla Società;
    - consulenza ai soggetti che hanno un contratto di collaborazione con APP Broker su tematiche di prodotto e/o di processo;
    - attività di *back office* e supporto nella gestione mandati.

3.1.1 Le attività in *outsourcing*

Per le attività di brokeraggio la Società si avvale del supporto di una società esterna (ARPA s.r.l.) con la quale è in essere apposito contratto di servizio.

Al medesimo *outsourcer*, è stata affidata lo svolgimento delle attività, in accordo a specifiche convenzioni, di consulenza, assistenza e prestazione di servizi relativamente a:

- prodotti assicurativi: progettazione e consulenza in merito ai prodotti assicurativi da proporre ai consumatori;
- gestione degli adempimenti e dei rapporti amministrativi e contabili della Società, inclusi anche i rapporti con gli Enti di Controllo;
- gestione contratti: incasso dei premi e controllo correttezza dei bonifici; input di emissione del contratto o della copertura a seguito della ricezione del bonifico; gestione amministrativa (anche relativamente alle provvigioni dei collaboratori); gestione estratti conto e regolazioni finanziarie; gestione del portafoglio e rinnovi delle polizze;
- *Information Technology*: lo sviluppo, l'implementazione e la manutenzione del software;
- liquidazione sinistri: gestione apertura istruttoria e gestione rapporti con la clientela..

Inoltre, per lo svolgimento delle proprie attività e nell'ottica di favorire economie di scala, APP Broker si avvale di strutture tecniche, operative e professionali della Capogruppo (o altre società di Service del Gruppo, per alcuni servizi IT), alla quale ha affidato, tramite la sottoscrizione di un apposito contratto di service, lo svolgimento dei seguenti servizi:

- contabilità generale, pianificazione e controllo di gestione: elaborazione dei dati e tenuta delle scritture contabili, nel rispetto delle disposizioni normative e dei principi contabili vigenti;
- segreteria societaria: assistenza all'attività degli organi sociali di APP Broker; corretta tenuta dei libri sociali; cura dei rapporti con soggetti esterni per gli adempimenti in materia societaria; consulenza in materia societaria;
- consulenza legale: consulenza in materie legali d'interesse per tutte le Società del Gruppo Allianz (e.g. Antiriciclaggio, Privacy); consulenza nella stesura di documenti contrattuali;

- servizi generali e acquisti: ricerca dei fornitori; valutazione delle offerte; ottenimento delle migliori condizioni d'acquisto; emissione ordini d'acquisto;
- attività relative agli adempimenti per la Legge 81 del 9/4/2008: gestione delle attività relative agli adempimenti in materia di salute e sicurezza;
- *Information Technology*: servizi di gestione applicativa e gestione dell'infrastruttura tecnologica; sviluppo software e manutenzione evolutiva. Si evidenza, infatti, che per la gestione e l'utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, APP Broker si avvale del supporto dell'U.O. IT Quality, Security & BCM di Allianz S.p.A., dei servizi offerti da Allianz technology S.c.p.A. alle consorziate.

3.2. Funzione e scopo del Modello

APP Broker è sensibile alle aspettative dei propri azionisti in quanto è consapevole del valore che agli stessi può derivare da un sistema di controllo interno idoneo a prevenire la commissione di comportamenti illeciti nel contesto aziendale.

Pertanto, l'adozione e l'efficace attuazione del Modello non solo consentono alla Società di beneficiare dell'esimente prevista dal D.lgs. 231/2001, ma migliorano la sua *Corporate Governance*, limitando il rischio di commissione di comportamenti illeciti.

I principi contenuti nel presente Modello devono condurre, da un lato, a determinare una piena consapevolezza nel potenziale autore del Reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi di APP Broker anche quando apparentemente essa potrebbe trarne un vantaggio); dall'altro, grazie ad un monitoraggio costante dell'attività, a reato stesso.

Scopo del Modello è pertanto la predisposizione di un sistema strutturato ed organico di prevenzione, dissuasione e controllo finalizzato alla riduzione del rischio di commissione dei Reati mediante la individuazione delle Attività Sensibili e, ove necessario, la loro conseguente proceduralizzazione.

In tale contesto si inserisce la costante attività dell'Organismo di Vigilanza finalizzata a garantire il rispetto del sistema organizzativo adottato e la vigilanza sull'operato dei destinatari, anche attraverso il ricorso ad idonei strumenti sanzionatori, sia disciplinari che contrattuali.

3.3. Natura e Fonti del Modello

Sebbene l'adozione del Modello sia prevista dal Decreto come facoltativa e non obbligatoria, in conformità alle sue politiche aziendali APP Broker ha ritenuto opportuno procedere all'adozione del Modello, con contestuale nomina dell'Organismo di Vigilanza.

Il MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO, approvato dal C.d.A. del 9/3/2015, costituisce regolamento interno di APP Broker vincolante per la medesima: esso è inteso come l'insieme delle regole operative e delle norme deontologiche adottate dalla Società – in funzione delle specifiche attività svolte – al fine di prevenire la commissione dei reati suscettibili di dare luogo ad una responsabilità dell'ente ai sensi del Decreto.

Il presente Modello è ispirato alle Linee Guida delle associazioni di categoria – in particolare delle Linee Guida A.N.I.A. – ed è fondato sulle risultanze della c.d. mappatura dei rischi.

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo esistenti e già ampiamente operanti nella Società, in quanto idonei a valere anche come misure di prevenzione dei Reati e di controllo sui processi coinvolti nelle Attività Sensibili.

Il presente Modello, ferma restando la sua funzione peculiare descritta al precedente paragrafo 3.2, si inserisce nel più ampio sistema di controllo esistente in Società, costituito principalmente dalle regole di *Corporate Governance* (compresi gli atti quali lo Statuto, le deleghe aziendali, le procure, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale, e, più in generale, tutte le procedure in essere). Tale sistema di controlli costituisce parte integrante del presente Modello.

Altri elementi che consentono di dare attuazione al Modello di APP Broker sono:

- le norme inerenti il sistema amministrativo, contabile, finanziario, di *reporting*;
- il Documento di Governo Societario;
- le comunicazioni e circolari aziendali al personale;
- la formazione del personale;
- le comunicazioni e circolari aziendali al personale;
- l'impianto procedurale implementato ai fini dell'ottenimento della certificazione BS OHSAS 18001:2007, relativa al sistema di gestione della Sicurezza e della Salute dei Lavoratori;
- il sistema sanzionatorio di cui ai CCNL;
- in generale, la normativa italiana e straniera applicabile.

Principi cardine cui il Modello si ispira, oltre a quanto sopra indicato ed al Codice Etico e di Comportamento (cfr. successivo par. 3.4), sono:

- le Linee Guida di categoria sopra richiamate, che hanno costituito elementi di riferimento costante in tutte le fasi di analisi e sviluppo del Modello;
- i requisiti indicati dal D.lgs. 231/2001 ed in particolare:
  - l'attribuzione ad un Organismo di Vigilanza (OdV) del compito di attuare in modo efficace e corretto il Modello, anche attraverso il monitoraggio dei comportamenti aziendali e il diritto ad una informazione costante sulle attività rilevanti ai fini del Decreto 231;
  - la messa a disposizione dell'OdV di risorse adeguate ai compiti affidatigli e ai risultati attesi e ragionevolmente ottenibili;
  - l'attività di verifica del funzionamento del Modello con conseguente aggiornamento periodico (controllo *ex post*);
  - l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;

- i principi generali di un adeguato sistema di controllo interno ed in particolare:
  - la verificabilità e documentabilità di ogni operazione rilevante ai fini del Decreto;
  - il rispetto del principio della separazione delle funzioni;
  - la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
  - la comunicazione all'OdV delle informazioni rilevanti;
  - il Codice Etico e di Comportamento. Le regole, procedure e principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello, ma fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare e sono costantemente aggiornati dalle funzioni aziendali a ciò preposte.

Per un maggior dettaglio sulle caratteristiche del sistema di controllo interno in essere, si rimanda al successivo capitolo 9 della Parte Speciale del presente Modello.

3.4. Codice Etico e di Comportamento e Modello

La Società, determinata a improntare lo svolgimento delle attività aziendali al rispetto della legalità, ha adottato il Codice Etico e di Comportamento del Gruppo Allianz S.p.A., con il quale quest'ultima ha inteso diffondere le linee guida alla conformità legale e alla condotta etica presso tutte le Società ed organizzazioni ad essa riconducibili.
Il Modello, le cui previsioni sono in ogni caso coerenti e conformi ai principi etici contenuti nei documenti sopra menzionati, risponde più specificamente alle esigenze espresse dal Decreto ed è, pertanto, finalizzato a prevenire la commissione delle fattispecie di reato ricomprese nell'ambito di operatività del D.lgs. 231/2001.
La documentazione in ambito etico afferma in ogni caso principi idonei a prevenire i comportamenti illeciti di cui al D.lgs. 231/2001, acquisendo pertanto rilevanza anche ai fini del Modello e costituendo un elemento ad esso complementare.

3.5. La costruzione del Modello e la sua struttura

La predisposizione del presente Modello è stata preceduta da una serie di attività preparatorie suddivise in differenti fasi e dirette tutte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D.lgs. 231/2001 ed ispirate oltre che alle norme in esso contenute anche alle Linee Guida di categoria.

Si riporta qui di seguito una breve descrizione di tutte le fasi in cui si è articolato il lavoro di individuazione delle aree a rischio, e sulle cui basi si è poi dato luogo alla predisposizione del presente Modello:

1. Identificazione delle Attività Sensibili ("*as-is analysis*")

L'identificazione delle Attività Sensibili è stata svolta attraverso la collaborazione dei soggetti chiave nell'ambito della struttura aziendale e l'esame della documentazione aziendale (organigrammi, attività svolte, processi principali, contratti, disposizioni organizzative, ecc.) e alcune interviste.

Dallo svolgimento di tale processo di analisi è stato possibile individuare, all'interno della struttura aziendale, una serie di Attività Sensibili e Strumentali nel compimento delle quali si potrebbe ipotizzare, quantomeno in astratto, l'eventuale commissione dei Reati.

I risultati di detta attività sono stati raccolti e formalizzati in uno specifico documento di analisi del profilo di rischio (anche "Matrice delle attività a rischio-reato"), che forma parte integrante del presente Modello e che illustra in dettaglio i profili di rischio relativi alla Società riguardanti la commissione dei reati ricompresi nel D.lgs. 231/2001.

In particolare, in detta mappatura sono dettagliate, per ogni famiglia / tipologia di reato, le aree aziendali a rischio di possibile commissione dei reati previsti dal D.lgs. 231/2001 (c.d. "Attività Sensibili"), gli esempi di possibili modalità e finalità di realizzazione di tali reati, nonché i processi nel cui svolgimento, sempre in linea di principio, potrebbero crearsi le condizioni e/o i mezzi per la commissione dei reati stessi (c.d. "processi sensibili").

La Mappatura delle attività a rischio-reato è custodita presso la Presidenza di APP Broker che ne cura l'archiviazione.

2. Effettuazione della *"gap analysis"*

Sulla base della situazione attuale (controlli e procedure esistenti in relazione alle Attività Sensibili) e delle previsioni e finalità del Decreto 231, si sono individuate le azioni di miglioramento dell'attuale sistema di controllo interno (processi e procedure esistenti) e dei requisiti organizzativi essenziali per la definizione di un Modello di organizzazione ai sensi del citato decreto.

L'attività appena descritta verrà effettuata ogni qual volta si rendesse necessario aggiornare e/o integrare il presente Modello.

3. Struttura del Modello.

Il presente Modello è costituito da una "Parte Generale" e da una "Parte Speciale" predisposta per le diverse categorie di reato contemplate nel D.lgs. 231/2001. La Parte Generale contiene le regole ed i principi generali del Modello. La Parte Speciale contiene, per ognuna delle tipologie di reato considerate, principi organizzativi e comportamentali volti a prevenire, o quanto meno limitare, la commissione di tali reati.

In particolare, la **Parte Generale** riporta:

- l'inquadramento normativo circa i contenuti del Decreto, i reati e gli illeciti amministrativi che determinano la responsabilità amministrativa dell'ente (cfr. Appendice 1) e le condizioni per l'esenzione della responsabilità;
- il modello di governo societario e di organizzazione e gestione della Società;
- le caratteristiche e le componenti essenziali del Modello, anche con specifico riferimento alle funzioni ed ai poteri dell'Organismo di Vigilanza (e connessi flussi informativi), al sistema sanzionatorio a presidio delle violazioni delle prescrizioni contenute nel Modello, alle modalità di comunicazione del Modello e di formazione del personale.

La **Parte Speciale**, articolata con riferimento ad ognuna delle famiglie di reato contemplate dal Decreto, che esplicita (per singola famiglia di reato):

- i reati della famiglia ritenuti astrattamente applicabili/rilevanti nel contesto organizzativo/operativo della Società;
- le attività sensibili con specifico riferimento all'operatività della Società;
- principi comportamentali e presidi organizzativi applicabili a tali attività sensibili.

4. Aggiornamento periodico e attività di *Risk Assessment*

Successivamente alla prima emanazione del modello, lo stesso è periodicamente aggiornato al fine di recepire eventuali modifiche normative o di natura organizzativa intervenute nel Gruppo Allianz S.p.A.

A tale scopo APP Broker S.r.l. svolge una serie di attività dirette sia all'aggiornamento del modello, nella sua parte generale e speciale, sia alla valutazione dei rischi di commissione dei reati al fine di identificare eventuali punti di miglioramento nell'ambito dei presidi di controllo definiti dalla Società.

Si riporta qui di seguito una breve descrizione delle fasi in cui si sostanzia l'attività di aggiornamento e *Risk Assessment*:

- mappatura, per ogni fattispecie di reato, all'interno di apposite matrici, delle attività sensibili, dei principi e delle procedure adottate dalla Società e poste a mitigazione del rischio di commissione dei reati ex D.lgs. n. 231/2001;
- condivisione delle schede e conduzione di apposite interviste con le diverse Funzioni coinvolte nelle attività sensibili mappate al fine di raccogliere:
    - riscontri circa la correttezza e la completezza, in base alle propria conoscenza ed esperienza, delle attività sensibili e dei presidi posti a mitigazione dei rischi reato, così come riportati nel Modello Organizzativo 231/2001;
    - indicazioni di modifiche/integrazioni intervenute nell'ambito dei presidi di controllo adottati dalla Società a fronte di ciascuna attività sensibile;
    - valutazione degli elementi di rischio di commissione del reato a cui è potenzialmente esposta ciascuna attività sensibile sulla base dell'esperienza e conoscenza dei soggetti coinvolti delle attività di business svolte;
- rielaborazione dei riscontri forniti al fine di:
    - recepire all'interno del Modello le eventuali modifiche o integrazioni indicate;
    - fornire una valutazione complessiva del rischio di commissione dei reati ex D.lgs 231 e identificare eventuali punti di miglioramento nell'ambito dei presidi di controllo definiti dalla Società.

3.6. La procedura di adozione e aggiornamento del Modello

Essendo il presente Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma I, lettera a del D.lgs. 231/2001), l'adozione dello stesso nonché le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione.

Il Modello è aggiornato tempestivamente, in tutto o in parte, anche su proposta dell'Organismo di Vigilanza, qualora intervengano mutamenti o modifiche:

a. nel sistema normativo e regolamentare che disciplina l'attività di APP Broker;

b. nella struttura o nell'organizzazione o articolazione di APP Broker;

c. nell'attività di APP Broker o dei suoi beni o servizi offerti alla clientela;

d. in riferimento ad altri e diversi elementi e circostanze essenziali e di diretto impatto sulle Attività Sensibili.

Le proposte di modifica al Modello sono preventivamente comunicate all'Organismo di Vigilanza, il quale deve tempestivamente esprimere un parere.

Qualora il Consiglio di Amministrazione ritenga di discostarsi dal parere dell'Organismo di Vigilanza, deve essere fornita adeguata motivazione.

3.7. Destinatari del Modello

Le regole contenute nel Modello si applicano a:

- a coloro che svolgono, anche di fatto, funzioni di rappresentanza, gestione, amministrazione, direzione o controllo della SOCIETÀ o di una unità o divisione di questa, dotata di autonomia finanziaria e funzionale (gli ESPONENTI AZIENDALI);
- ai lavoratori subordinati della SOCIETÀ, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale (i DIPENDENTI);

- a chi, pur non appartenendo alla SOCIETÀ, opera su mandato o nell'interesse della medesima;
- ai COLLABORATORI e controparti contrattuali in generale.

Il Modello costituisce riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività che interessano APP Broker.

Nei contratti con Consulenti dovrà pertanto essere inserita una clausola con cui gli stessi dichiarino di essere a conoscenza dell'avvenuta adozione del Modello da parte di APP Broker e di aver preso visione del medesimo e del Codice Etico e di Comportamento, impegnandosi al rispetto dei principi ivi contenuti.

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

Il Modello di APP Broker è messo a disposizione con le modalità indicate nel precedente paragrafo 3.6.

CAPITOLO 4 – LE ATTIVITA' SENSIBILI DI APP BROKER

4.1 Le Attività Sensibili di APP BROKER

A seguito dell'analisi del contesto aziendale condotta da APP Broker, è emerso che le attività sensibili al rischio *ex* D.lgs. 231/2001, riguardano le seguenti fattispecie di reato:

a) *Reati nei rapporti con la P.A (art. 24 e 25 del Decreto);*

b) *Delitti informatici e trattamento illecito dei dati (art. 24 bis del Decreto);*

c) *Delitti di criminalità organizzata (art. 24 ter del Decreto);*

d) *Reati societari (inclusivi del reato di Corruzione tra privati) (art. 25 ter Decreto);*

e) *Delitti con finalità di terrorismo (art. 25 quater Decreto);*

f) *Reati di omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 septies Decreto);*

g) *Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè di autoriciclaggio (art. 25 octies Decreto);*

h) *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies Decreto);*

i) *Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies Decreto);*

j) *Delitti contro la personalità individuale, con esclusivo riferimento alla fattispecie di cui al rinnovato art. 603-bis del Codice Penale, "Intermediazione illecita e sfruttamento del lavoro".*

Il rischio relativo agli altri reati contemplati dal D.Lgs. 231/2001 non appare al momento concretamente ipotizzabile. Per il dettaglio delle attività ritenute sensibili in relazione alle famiglie di reato sopra elencate, si rimanda a quanto descritto nella Parte Speciale del presente Modello.

Come precedentemente indicato, in generale occorre rilevare che molte delle attività che potrebbero astrattamente condurre alla commissione di uno dei reati previsti dal D.Lgs. 231/2001 sono in realtà presidiate e/o svolte, attraverso specifici contratti di outsourcing, da ciascuna delle competenti funzioni di Allianz e da Arpa S.r.l..

In considerazione di ciò, pertanto, tali attività possono essere considerate come adeguatamente presidiate anche dal Modello di Allianz (che ricomprende anche le attività svolte da Sistemi Informativi Allianz).

Resta fermo il potere dell'OdV di individuare eventuali ulteriori attività a rischio che – a seconda dell'evoluzione legislativa o dell'attività di APP Broker – potranno essere ricomprese nel novero delle Attività Sensibili.

CAPITOLO 5 – PRESTAZIONI DI SERVIZI SVOLTE DA ALTRE SOCIETÀ DEL GRUPPO IN FAVORE DELLA SOCIETÀ

La prestazione di servizi infragruppo avviene nel rispetto dei seguenti principi:

- obbligo che tutti i contratti infragruppo siano stipulati per iscritto e che della suddetta stipulazione sia dato avviso all'Organismo di Vigilanza della Società, il quale potrà nel caso prenderne visione;
- obbligo reciproco tra la società beneficiaria e quella che rende il servizio di rendere noto al proprio Organismo di Vigilanza e all'Organismo di Vigilanza dell'altra società, eventuali criticità rilevanti ai fini 231 che interessino il servizio reso;
- obbligo per la società che rende il servizio e per la beneficiaria del medesimo di attenersi al proprio Modello 231 e al Codice Etico e di Comportamento.

Resta ferma l'applicazione, per quanto rilevante, della "policy in materia di esternalizzazioni" adottata a livello di gruppo come da suo ultimo aggiornamento.

CAPITOLO 6 – ORGANISMO DI VIGILANZA (OdV)

6.1 Identificazione dell'organismo di vigilanza

In base alle previsioni dell'art. 6, comma 1, lett. a) e b) del Decreto, l'Ente può essere esonerato dalla responsabilità conseguente alla commissione di illeciti da parte dei soggetti qualificati ex art. 5 del Decreto, se l'organo dirigente ha, fra l'altro:

- adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento ad un Organismo della Società dotato di autonomi poteri di iniziativa e controllo.

L'affidamento a tale Organismo dei suddetti compiti, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, i presupposti indispensabili per l'esonero dalla responsabilità prevista dal Decreto.
Il compito di vigilare sul funzionamento, l'aggiornamento e la concreta applicazione del Modello è affidato ad un Organismo di Vigilanza (OdV).

In assenza di riferimenti normativi, la concreta costituzione dell'Organismo di Vigilanza - che di fatto esercita un potere, da un lato, di prevenzione e, dall'altro, di controllo e intervento - è rimessa all'iniziativa organizzativa della Società, sempre in funzione del quadro delineato dal Decreto.

In base alle previsioni del D.lgs. 231/2001, l'organismo cui affidare il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento, deve essere un organismo della società (art. 6.1, *b)* del D.lgs. 231/2001), dotato di autonomi poteri di iniziativa e controllo.

A tal fine l'OdV deve essere dotato delle seguenti caratteristiche:

- **autonomia e indipendenza:** il requisito di autonomia e indipendenza presuppone che l'OdV riferisca, per l'effettivo svolgimento delle sue funzioni, solo al massimo vertice gerarchico cioè al Consiglio di Amministrazione (di seguito anche "C.d.A.") e non operi alle dipendenze ed in base alle direttive di alcuna altra funzione, né dell'alta direzione, né dell'organo decisionale. In

proposito, sempre le Linee Guida indicano come rilevante l'istituzione di un canale di comunicazione tra l'organismo di vigilanza e l'organo decisionale (nel caso del C.d.A., questo nel suo insieme), con la società incaricata della revisione dei bilanci e con il Responsabile del Servizio di prevenzione e protezione.

L'OdV dispone di autonomi poteri di spesa sulla base di un preventivo annuale, approvato dal C.d.A. nel contesto di formazione del budget aziendale, su proposta dell'OdV stesso, di stanziamento di una dotazione adeguata di risorse finanziarie, della quale potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte, ecc.). Inoltre, l'OdV può autonomamente impegnare risorse che eccedono i propri poteri di spesa, qualora l'impiego di tali risorse sia necessario per fronteggiare situazioni eccezionali ed urgenti. In questi casi l'OdV deve informare il C.d.A. alla prima riunione utile.
L'indipendenza infine presuppone che i componenti dell'Organismo di Vigilanza non si trovino in una posizione, neppure potenziale di conflitto d'interessi con la Società, né siano titolari all'interno della stessa di funzioni di tipo operativo.

- **Comprovata professionalità, capacità specifiche in tema di attività ispettiva e consulenziale** per garantirne le capacità di azione. L'Organismo di Vigilanza possiede, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio; è necessario, pertanto, che all'interno dell'Organismo di Vigilanza siano presenti soggetti con professionalità adeguate in materia economica e di controllo e gestione dei rischi aziendali. L'Organismo di Vigilanza potrà, inoltre, anche avvalendosi di professionisti esterni, dotarsi di risorse competenti in materia giuridica di organizzazione aziendale, revisione, contabilità e finanza.
- **Continuità di azione** al fine di garantire la costante attività di monitoraggio e di aggiornamento del Modello e la sua variazione al mutare delle condizioni aziendali di riferimento. L'Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine; è una struttura riferibile alla società, in modo da garantire la dovuta continuità nell'attività di vigilanza; cura l'attuazione del Modello assicurandone il costante aggiornamento; non svolge mansioni operative che possano condizionare e contaminare quella visione d'insieme sull'attività aziendale che ad esso si richiede.

Applicando tutti i principi citati alla realtà aziendale di APP Broker, ed in considerazione delle osservazioni da parte del Ministero della Giustizia in merito ai contenuti delle Linee Guida con riguardo alle caratteristiche soggettive e oggettive dell'OdV, nonché della specificità dei compiti che fanno capo allo stesso, contestualmente all'approvazione del presente modello, la Società istituisce l'OdV nella forma di un organismo monocratico assegnato a un membro esterno.

Tale scelta è stata determinata dal fatto che la suddetta figura è stata riconosciuta come la più adeguata ad assumere il ruolo dell'OdV in quanto, oltre ai requisiti di autonomia, indipendenza, professionalità, onorabilità e continuità d'azione che si richiedono per tale funzione, possiede altresì quei requisiti soggettivi formali che garantiscono ulteriormente l'autonomia e l'indipendenza richiesta dal compito affidato, quali l'assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.

L'OdV così costituito provvede a darsi le proprie regole di funzionamento attraverso un specifico regolamento dell'OdV.

L'OdV si può avvalere del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

Il conferimento dell'incarico all'OdV e la revoca del medesimo (ad es. in caso violazione dei propri doveri derivanti dal Modello) sono atti riservati alla competenza del C.d.A..

La revoca di tale incarico sarà ammessa, oltre che per giusta causa (ad esempio, infedeltà, inefficienza, negligenza, ecc.), anche nei casi di impossibilità sopravvenuta ovvero allorquando vengano meno in capo al componente dell'OdV i requisiti di indipendenza, imparzialità, autonomia, i requisiti di onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.

6.2 Funzione e poteri dell'OdV

All'OdV è affidato il compito di vigilare:

- sull'osservanza del Modello da parte di tutti i Destinatari;

- sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative, sollecitando a tal fine gli organi competenti.

Più specificamente, all'OdV sono altresì affidati i seguenti compiti di:

i. Verifiche e controlli:

   a. sollecitare l'attuazione delle procedure di controllo previste dal Modello anche tramite l'emanazione o proposizione di disposizioni (normative e/o informative) interne;

   b. condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle Attività Sensibili anche per quanto attiene alla valutazione del rischio rilevante;

   c. effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere dalle Società di Service in esecuzione dei contratti di servizio in essere con APP Broker, i cui risultati devono essere riassunti in un'apposita relazione periodica da esporsi in sede di *reporting* al Consiglio di Amministrazione;

   d. raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere a lui trasmesse o tenute a sua disposizione;

   e. coordinarsi con le altre funzioni aziendali - e con le funzioni aziendali di Allianz che effettuano attività per conto di APP Broker in esecuzione di appositi contratti di servizio - (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello. A tal fine, l'OdV ha accesso a tutta la documentazione aziendale che ritiene rilevante e deve essere costantemente informato dalle funzioni aziendali competenti o dalle funzioni di Allianz che svolgono per la stessa determinate attività in esecuzione di appositi contratti di servizio: - sugli aspetti dell'attività aziendale che possono esporre la Società al rischio di commissione di uno dei Reati; - sui rapporti con le Società di Service, sub-Agenti e Consulenti che operano per conto di APP Broker nell'ambito delle Attività Sensibili;

f. attivare e svolgere le indagini interne a seguito di segnalazioni ricevute.

ii. Formazione ed informazione:

a. coordinarsi con le funzioni competenti per la definizione dei programmi di formazione per il personale e del contenuto delle comunicazioni periodiche da inviare ai Dipendenti, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.lgs. 231/2001;

b. monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso.

iii. Sanzioni:

a. coordinarsi con le funzioni competenti per valutare l'adozione di eventuali sanzioni o provvedimenti, fermo restando le competenze delle stesse per l'irrogazione della misura adottabile e il relativo procedimento decisionale (si rinvia in merito a questo punto al successivo capitolo 8).

iv. Aggiornamenti:

a. interpretare la normativa rilevante in coordinamento con la Funzione Compliance di gruppo e Affari Legali di Allianz e verificare l'adeguatezza del Modello a tali prescrizioni normative;

b. valutare le esigenze di aggiornamento e adeguamento del Modello, anche attraverso apposite riunioni con le varie funzioni aziendali interessate e con quelle di Allianz S.p.A. che esercitano attività per conto di APP Broker in esecuzione dei diversi contratti di servizio;

c. monitorare l'aggiornamento dell'organigramma aziendale, ove è descritta l'organizzazione dell'ente nel suo complesso con la specificazione delle aree, strutture e uffici, e relative funzioni.

Clausola generale

L'OdV ha, come previsto dalla legge, autonomi poteri di iniziativa e controllo al fine di vigilare sul funzionamento e l'osservanza del Modello, ma non ha poteri coercitivi o di intervento modificativi della

struttura aziendale o sanzionatori nei confronti dei Destinatari, poteri questi che sono demandati agli organi o funzioni aziendali competenti.

6.3 L'attività di *reporting* dell'OdV verso altri organi aziendali

L'OdV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità, sulla base delle seguenti linee di *reporting*:

- su base annuale e avente ad oggetto l'attività di volta in volta posta in essere, direttamente verso il Consiglio di Amministrazione;
- qualora venga a conoscenza di fatti di particolare gravità o significatività imputabili a componenti del Consiglio di Amministrazione ne farà tempestivo rapporto al Collegio Sindacale.

L'OdV predispone nello specifico:

1) annualmente una relazione descrittiva per il C.d.A., sull'attività svolta nel corso del periodo, in cui vengono evidenziati i controlli effettuati e i relativi esiti, le criticità rilevate, nonché l'eventuale necessità di aggiornamento delle Attività Sensibili;

2) al termine del secondo bimestre di ciascun anno, trasmette al C.d.A. un piano delle attività di verifica e controllo per l'anno successivo.

Qualora l'OdV rilevi criticità riferibili a qualcuno degli organi sopraindicati, la corrispondente segnalazione è da destinarsi prontamente a uno degli altri organi.

L'attività di reporting ha in ogni caso sempre ad oggetto:

- formulazione delle proposte per gli eventuali aggiornamenti ed adeguamenti del Modello e del Codice Etico e di Comportamento adottati;

- violazioni accertate del Modello e del Codice Etico e di Comportamento affinché vengano presi gli opportuni provvedimenti;
- attività svolte (comprese ad esempio le attività di formazione), verifiche e controlli compiuti, nonché esito dei medesimi ed eventuali criticità emerse in termini di comportamenti o eventi che possono avere un effetto sull'adeguatezza o sull'efficacia del Modello e del Codice Etico e di Comportamento.

Gli incontri con gli Organi cui l'OdV riferisce devono essere verbalizzati e copie dei verbali devono essere custodite dall'OdV e dagli organismi di volta in volta coinvolti.

L'Organismo di Vigilanza può essere convocato in qualsiasi momento dal Consiglio di Amministrazione di APP Broker e, a propria volta, può richiedere di essere da quest'ultimo sentito qualora ravvisi l'opportunità di riferire su questioni inerenti il funzionamento e l'efficace attuazione del Modello o in relazione a situazioni specifiche.

A garanzia di un corretto ed efficace flusso informativo, nonché al fine di un completo e corretto esercizio dei propri compiti, l'Organismo ha inoltre facoltà di richiedere chiarimenti o informazioni direttamente ai soggetti con le principali responsabilità operative.

L'OdV deve, inoltre, coordinarsi con le funzioni competenti presenti nel Gruppo per i diversi profili specifici e precisamente:

- con la funzione Affari Legali di Allianz (ad esempio, per l'interpretazione della normativa rilevante, per la modifica o integrazione della mappatura delle Attività Sensibili, per determinare il contenuto delle clausole contrattuali);
- con la Segreteria Societaria per gli adempimenti societari che possono avere rilevanza ai fini della commissione dei reati societari;
- con il Servizio di Prevenzione e Protezione, per gli adempimenti che possono avere rilevanza in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- con la funzione Risorse Umane in ordine alla formazione del personale e ad eventuali procedimenti disciplinari;
- con l'Unità Internal Audit di Gruppo per il monitoraggio dei risultati dell'attività svolta ai sensi del D.Lgs. 231/2001 e l'integrazione dell'attività futura.

L'Organismo di Vigilanza può pianificare incontri periodici con i Responsabili delle Funzioni Aziendali sopra citate, nel proprio programma di Attività annuale o previsti a evento, qualora ritenuto necessario.

6.4 Obblighi di informazione nei confronti dell'OdV

L'OdV deve essere prontamente informato in merito ai fatti di gestione posti in essere nell'ambito delle Attività Sensibili che potrebbero esporre la Società al rischio di commissione di Reati ex D.lgs. 231/2001.

Al fine di tenere costantemente monitorate le Attività Sensibili, l'OdV si avvale di un sistema di flussi informativi e di segnalazioni provenienti da:

- funzioni che operano in aree aziendali a rischio di commissione di Reati ex D.lgs. 231/2001;
- funzioni di controllo (Internal Audit di Gruppo, Compliance di Gruppo e Risk Management);
- altre funzioni in possesso di dati e informazioni in grado di supportare l'OdV nello svolgimento della propria attività di vigilanza;
- Organi Sociali (Consiglio di Amministrazione, Collegio Sindacale e Comitato Consultivo in materia di Controlli Interni).

L'Organismo di Vigilanza può pianificare incontri periodici con i Responsabili delle Funzioni Aziendali sopra citate, nel proprio programma di Attività annuale o previsti a evento, qualora ritenuto necessario.

La Società ha adottato la *"Procedura flussi informativi verso l'Organismo di Vigilanza ex D.lgs. 231/2001"* che disciplina le tipologie e le tempistiche di trasmissione dei flussi informativi verso l'OdV da parte di ciascuna funzione e organo societario.

In particolare, la predetta procedura disciplina a livello aziendale:

1) i flussi informativi periodici verso l'OdV: la procedura individua per ciascuna funzione aziendale ivi considerata, la tipologia di flussi e la relativa periodicità di trasmissione all'OdV. Tali flussi possono consistere nella trasmissione di report o documenti o in incontri periodici con l'OdV stesso.

2) Segnalazioni all'OdV: flussi informativi estemporanei, trasmessi all'OdV in occasione del verificarsi di fatti o comportamenti in violazione, sospetto di violazione o elusione del Modello o delle procedure di attuazione dello stesso.

La *"Procedura flussi informativi verso l'Organismo di Vigilanza ex D.lgs. 231/2001"* disciplina inoltre: a) le modalità di trasmissione dei flussi informativi e delle segnalazioni all'OdV; b) l'analisi dei flussi e delle segnalazioni ricevute; e c) l'archiviazione delle informazioni e dei documenti ricevuti.

Tutti i Destinatari del presente Modello sono quindi tenuti a segnalare all'OdV qualsiasi comportamento, tenuto nell'ambito delle attività aziendali e/o comunque nell'interesse della Società, che possa configurare, direttamente o indirettamente, una violazione del Modello stesso o un reato ex D.lgs. 231/2001.

In particolare, i Dirigenti, i Responsabili di Funzione e i Dipendenti sono tenuti a segnalare tutte le tipologie di informazioni espressamente previste nel paragrafo 6.1 della *"Procedura flussi informativi verso l'Organismo di Vigilanza ex D.lgs. 231/2001".*

Nel caso in cui all'OdV pervengano segnalazioni non attinenti, lo stesso provvede a trasmetterle alle funzioni di volta in volta competenti.

In ogni caso, qualora uno dei suddetti soggetti non adempia agli obblighi informativi sopra menzionati, allo stesso sarà irrogata una sanzione disciplinare che varierà a seconda della gravità dell'inottemperanza agli obblighi sopra menzionati e che sarà comminata secondo le regole indicate nel paragrafo 7 del presente Modello. L'OdV si riserva di segnalare agli Organi Sociali o alle funzioni competenti l'opportunità di agire contro chiunque effettui in malafede segnalazioni non veritiere.

Nello specifico, i Destinatari devono riferire all'Organismo di Vigilanza, a tutela dell'integrità della Società, effettuando segnalazioni circostanziate di condotte illecite rilevanti ai sensi del Decreto e fondate su elementi di fatto, per quanto possibile, precisi e concordanti, o su violazioni del presente Modello, di cui siano venuti a conoscenza.

A tal fine, sono istituiti, e resi noti a tutti i Destinatari del presente Modello, canali dedicati per la consultazione dell'Organismo di Vigilanza (si v. infra "*Modalità delle segnalazione*"), attraverso i quali potranno essere inviate le eventuali segnalazioni, anche nel rispetto di quanto previsto dall'art. 6, co. 2-bis del Decreto 231 in materia di whistleblowing.

L'accesso alle segnalazioni ricevute tramite tali canali è riservato all'Organismo di Vigilanza, personalmente o per il tramite di delegati.

Tutte le modalità di segnalazione garantiscono l'opportuna riservatezza dell'identità dei segnalanti, anche al fine di evitare atteggiamenti ritorsivi o qualsiasi forma di discriminazione o penalizzazione nei loro confronti. La Società, infatti, garantisce la tutela dei soggetti segnalanti contro qualsiasi forma, diretta o indiretta, di ritorsione, discriminazione, penalizzazione, applicazione di misure sanzionatorie, demansionamento, licenziamento, trasferimento o sottoposizione ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro per motivi collegati, direttamente o indirettamente, alla segnalazione.

La Società assicura in tutti i casi la riservatezza e l'anonimato del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

I Consulenti, gli Intermediari Assicurativi e i Partner sono contrattualmente tenuti a segnalare alla Società il coinvolgimento in uno dei Reati di cui al D.lgs. 231/2001.

Modalità delle segnalazioni

Tutte le segnalazioni, di dipendenti della Società, di agenti e loro collaboratori ed in genere di tutti i soggetti che abbiano qualsiasi tipo di relazione con la Società, che abbiano ad oggetto l'evidenza o il sospetto di violazione del Modello o la commissione di reati ex D.lgs. 231/2001 vanno inviate all'Organismo di Vigilanza utilizzando prioritariamente l'indirizzo di posta elettronica Organismodivigilanza-231-appbroker@allianz.it

Qualora i segnalanti fossero impossibilitati a procedere con la modalità di segnalazione ora descritta, i relativi flussi potranno essere trasmessi per iscritto alla Casella Postale:

APP Broker S.r.l. - Organismo di Vigilanza ai sensi del D.lgs. 231/2001

c/o Studio Legale Guasti nella persona del Notaio Francesco Guasti

Piazza Paolo Ferrari, 8

20121 Milano

Tutte le segnalazioni inviate all'indirizzo sopra indicato saranno trasmesse in via riservata all'Organismo di Vigilanza, il quale avrà accesso, personalmente o per il tramite di delegati, ai relativi contenuti.

Le segnalazioni potranno essere inviate anche in forma anonima, all'Organismo di Vigilanza utilizzando l'applicativo presente nel portale aziendale riservato ai dipendenti, o nel sito internet delle Società stesse.

L'OdV valuta le segnalazioni ricevute e dà ad esse seguito secondo la "Procedura flussi informativi verso l'Organismo di Vigilanza ex D.lgs. 231/2001"; gli eventuali provvedimenti conseguenti sono applicati dalle competenti funzioni aziendali in conformità a quanto previsto al successivo capitolo 7 (Sistema sanzionatorio).

L'OdV non è tenuto a prendere in considerazione le segnalazioni anonime che appaiano prima facie irrilevanti, destituite di fondamento o non circostanziate.

6.6 Verifiche sull'adeguatezza del Modello

Oltre all'attività di vigilanza che l'OdV svolge continuamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti dei destinatari ed il Modello stesso), esso periodicamente effettua, con cadenza almeno annuale specifiche verifiche sulla reale capacità del Modello di prevenire i Reati, coordinandosi con soggetti terzi con adeguate caratteristiche di professionalità ed indipendenza.

Inoltre, viene svolta una *review* di tutte le segnalazioni ricevute nel corso dell'anno, delle verifiche a campione degli eventi considerati rischiosi e della sensibilizzazione dei Dipendenti e degli Organi Sociali rispetto alla problematica della responsabilità penale dell'impresa.

Per le verifiche l'OdV si avvale, di norma, delle funzioni interne ed esterne che si rendano a tal fine necessarie.

Le verifiche e il loro esito sono inserite nella relazione semestrale nei confronti del Consiglio di Amministrazione. In particolare, in caso di emersione di criticità, l'OdV esporrà i miglioramenti da attuare.

6.7 Raccolta e conservazione delle informazioni

Tutte le informazioni, la documentazione ivi compresa la reportistica prevista dal Modello, e le segnalazioni raccolte dall'Organismo di Vigilanza (ed allo stesso pervenute) nell'espletamento dei propri compiti istituzionali, sono conservate a cura dell'OdV in un apposito database (informatico o cartaceo) per un periodo di almeno 10 anni

CAPITOLO 7 – FORMAZIONE E DIFFUSIONE DEL MODELLO

Ai fini dell'efficacia del presente Modello, è obiettivo di APP Broker garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute sia nei confronti di tutti Destinatari (sia Dipendenti sia collaboratori, Società di Service). Tale obiettivo riguarda tutte le risorse aziendali che rientrano nelle categorie anzidette, sia che si tratti di risorse già presenti in azienda sia che si tratti di quelle da inserire. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle Attività Sensibili.

L'attività di **informazione** concernente i contenuti ed i principi del Modello, diversamente caratterizzata a seconda dei **Destinatari** cui essa si rivolge, è improntata a completezza, tempestività, accuratezza e continuità, al fine di consentire la piena consapevolezza delle disposizioni aziendali che i Destinatari stessi sono tenuti a rispettare.

Gli strumenti che la Società adotta per effettuare una comunicazione efficace del Modello sono i seguenti:

- i contenuti ed i principi del Modello sono portati a conoscenza dei Dipendenti, mediante intranet aziendale.

- un estratto del Modello (unitamente al Codice Etico e di Comportamento) è fornito e/o messo a disposizione di soggetti che intrattengono rapporti di collaborazione contrattualmente regolati e coinvolti nello svolgimento di attività sensibili, con particolare attenzione a quanti sono soggetti alla direzione o alla vigilanza. In questo caso i contratti e le lettere di incarico prevedono clausole di "non violazione del Modello di organizzazione, gestione e controllo della Società" i Collaboratori il cui rapporto con APP Broker è già in essere al momento dell'adozione del Modello, viene inviata una comunicazione di avvenuta adozione del Modello da parte di APP Broker con invito a rispettarne i contenuti;

- è data facoltà ai dipendenti di contattare l'Organismo di Vigilanza per eventuali chiarimenti sui comportamenti da adottare al fine di rispettare i principi enunciati nel Modello adottato.

Le specifiche attività di **formazione** nei confronti del **personale** devono prevedere diversi livelli di approfondimento in ragione del differente grado di coinvolgimento del personale nelle attività a rischio-reato ed in relazione ai rispettivi ambiti di operatività e responsabilità. In particolare, l'attività di formazione deve coinvolgere tutto il personale in forza, nonché le risorse di volta in volta inserite nell'organizzazione aziendale anche in relazione ad evoluzioni organizzative interne e normative.

La partecipazione ai programmi di formazione sopra descritti è obbligatoria e il controllo circa l'effettiva frequenza è demandata, sulla base di specifico contratto di servizio, alla Funzione Risorse Umane di Allianz, che ne relaziona all'OdV.

La mancata partecipazione non giustificata ai programmi di formazione comporterà l'irrogazione di una sanzione disciplinare che sarà comminata secondo le regole indicate nel capitolo 8 del presente Modello.

CAPITOLO 8 – SISTEMA SANZIONATORIO

8.1 Funzione del sistema sanzionatorio

Il Decreto richiede che il Modello introduca un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso. Tale sistema sanzionatorio costituisce inoltre, ai sensi dell'art. 6 , co. 1, lett. e) del D.lgs. 231/2001, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità dell'ente. Inoltre, a seguito della citata Legge n. 179/2017 in materia di whistleblowing, il legislatore ha stabilito che nel suddetto sistema disciplinare, devono essere espressamente previste «sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate (art. 6, co. 2-bis, lett. d) del D.lgs. 231/2001).

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di deterrenza) applicabili in caso di violazione delle regole di cui al presente Modello, rende efficiente l'azione di vigilanza dell'OdV ed ha lo scopo di garantire l'effettività del Modello stesso.

Il presupposto ulteriore per l'effettività del Modello è che ogni ipotesi di violazione sia portata all'attenzione dell'OdV e riceva un adeguato seguito.

L'applicazione del sistema sanzionatorio presuppone la semplice violazione delle disposizioni del Modello e del Codice Etico e di Comportamento; pertanto essa verrà attivata indipendentemente dallo svolgimento e dall'esito del procedimento penale, eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.lgs. 231/2001.

L'applicazione delle misure sanzionatorie non pregiudica né modifica ulteriori, eventuali conseguenze civilistiche o di altra natura (penale, amministrativa, tributaria), che possano derivare dal medesimo fatto.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare. Il sistema disciplinare

non solo è autonomo rispetto all'eventuale azione penale, ma anzi deve rimanere su un piano nettamente distinto e separato dal sistema normativo del diritto penale ed amministrativo. Nel caso in cui APP Broker preferisca comunque attendere l'esito del giudizio penale, essa potrà ricorrere all'istituto dell'allontanamento temporaneo del servizio e rinviare alle risultanze anche non definitive del giudizio penale l'eventuale avvio di un procedimento disciplinare.

Ogni violazione o elusione del Modello o delle procedure di attuazione dello stesso, da chiunque commessa, deve essere immediatamente comunicata, per iscritto, all'Organismo di Vigilanza, ferme restando le procedure e i provvedimenti disciplinari che restano di esclusiva competenza del titolare del potere disciplinare.

Tutti i Destinatari del Modello hanno il dovere di effettuare le suddette segnalazioni.

L'OdV deve essere immediatamente informato dell'applicazione di una sanzione, per violazione del Modello o delle procedure stabilite per la sua attuazione, disposta nei confronti di qualsivoglia soggetto tenuto all'osservanza del Modello e delle procedure prima richiamate.

-Inoltre, con riferimento al sistema sanzionatorio relativo alla corretta gestione delle segnalazioni di illeciti ai sensi dell'art. 6, co. 2-bis, D.lgs. 231/2001, nei confronti di tutti i Destinatari del presente Modello sono previste:

- sanzioni a tutela del segnalante per chi pone in essere atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante stesso per motivi collegati, direttamente o indirettamente, alla segnalazione; e

- sanzioni nei confronti di chi effettua, con dolo o colpa grave, segnalazioni che si rivelano infondate.

Le sanzioni sono definite in relazione al ruolo del Destinatario delle stesse, secondo quanto indicato dai successivi paragrafi, nella misura in cui le violazioni delle norme relative al sistema di segnalazione rappresentino, esse stesse, delle violazioni delle disposizioni del presente Modello.

8.2 Misure nei confronti dei Dipendenti

La violazione da parte dei Dipendenti soggetti al CCNL delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.

A. Dipendenti che non rivestono la qualifica di dirigenti

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) e delle eventuali normative speciali applicabili - sono quelli previsti dall'apparato sanzionatorio di cui al CCNL applicato da APP Broker:

- rimprovero verbale;
- biasimo inflitto per iscritto;
- sospensione dal servizio e dal trattamento economico, nei limiti stabiliti all'art. 25 CCNL;
- licenziamento (nei casi previsti dalla legge nonché in quelli previsti dal Codice Disciplinare in vigore).

Restano ferme - e si intendono qui richiamate – tutte le disposizioni, previste dalla legge e dai Contratti Collettivi applicati, relative alle procedure e agli obblighi da osservare nell'applicazione delle sanzioni.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, agli organi e funzioni che risultano in tal senso competenti; questi ultimi agiranno dando informativa contestuale al Consiglio di Amministrazione.

Fermi restando gli obblighi per APP Broker nascenti dallo Statuto dei Lavoratori e dal Contratto Collettivo e dai regolamenti interni applicabili, i comportamenti sanzionabili riguardano:

- l'adozione, nell'espletamento delle Attività Sensibili, di comportamenti in violazione delle prescrizioni del presente Modello, ovvero
- violazione di procedure interne eventualmente richiamate dal Modello stesso tali da poter determinare la concreta applicazione a carico di APP Broker di sanzioni previste dal D.lgs. 231/2001.

B. Dipendenti che rivestono la qualifica di dirigenti

In caso di violazione, da parte di dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento delle Attività Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, la Società provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto normativamente previsto.

Fermi restando gli obblighi per APP Broker nascenti dal Contratto Collettivo e dai regolamenti interni applicabili, i comportamenti sanzionabili riguardano:

- l'adozione, nell'espletamento delle Attività Sensibili, di comportamenti in violazione delle prescrizioni del presente Modello e diretti in modo univoco al compimento di uno o più Reati riconducibili ad APP Broker, ovvero
- violazione di procedure interne previste dal Modello tali da poter determinare la concreta applicazione a carico di APP Broker di sanzioni previste dal D.lgs. 231/2001.

Per quanto riguarda l'accertamento delle infrazioni e l'irrogazione delle sanzioni restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, agli organi societari e funzioni aziendali competenti.

* * *

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate al livello di responsabilità ed autonomia del dipendente e del dirigente, all'eventuale esistenza di precedenti disciplinari a carico degli stessi, all'intenzionalità del comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui APP Broker può ragionevolmente ritenersi esposta - ai sensi e per gli effetti del D.lgs. 231/2001 - a seguito della condotta censurata.

Più specificamente, il tipo e l'entità di ciascuna delle sanzioni sopra richiamate saranno applicate in relazione:

- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia anche con riguardo alla prevedibilità dell'evento;
- al comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o

meno di precedenti disciplinari del medesimo nei limiti consentiti dalla legge;

- alle mansioni del lavoratore;
- alla posizione funzionale delle persone coinvolte nei fatti costituenti mancanza;
- altre particolari circostanze che accompagnano la violazione disciplinare.

Resta sempre salvo il risarcimento di ogni danno arrecato ad APP Broker.

8.3 Misure nei confronti dei Soggetti Apicali

La violazione dello specifico obbligo di vigilanza sui sottoposti gravante sui soggetti apicali che ricoprono funzioni di amministrazione e rappresentanza comporterà l'assunzione, da parte della Società, delle misure sanzionatorie ritenute più opportune in relazione, da una parte, alla natura e gravità della violazione commessa e, dall'altra, alla qualifica dell'apicale in oggetto.

8.4 Misure nei confronti dei Consulenti e altri soggetti esterni (subagenti)

Ogni violazione delle regole di cui al presente Modello applicabili ai Consulenti, e a ogni altro soggetto esterno che opera per conto di / collabora con APP Broker, ovvero ogni commissione dei Reati previsti dal Modello è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

Resta, in ogni caso, salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti ad APP Broker, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal D.lgs. 231/2001.

PARTE SPECIALE

CAPITOLO 9 – PRINCIPI GENERALI DELLA PARTE SPECIALE

9.1. Premessa

In conformità all'art. 6 del Decreto, il sistema dei controlli interni deve prevedere, in relazione ai reati da prevenire: *i)* specifici protocolli per programmare la formazione e l'attuazione delle decisioni societarie; *ii)* l'individuazione di modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.

Le procedure sono costantemente aggiornate, anche su proposta o segnalazione dell'OdV.

L'OdV verifica che le procedure siano idonee al rispetto dei principi contenuti nel Modello.

L'OdV propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle procedure di attuazione.

L'OdV concorre a definire, con le funzioni aziendali interessate, le operazioni di carattere *significativo* alle quali si applicano le procedure ispirate ai principi del Modello.

Sono indici di *significatività* dell'operazione: il suo valore e portata economica in riferimento all'attività aziendale nel comparto interessato, la sua incidenza sui processi decisionali e produttivi, la sua rilevanza rispetto alla ordinaria attività di impresa.

Sono ammesse, nei casi di particolare urgenza o in caso di impossibilità temporanea di rispetto delle procedure, sotto la responsabilità di chi le attua, eventuali deroghe a quanto previsto nella presente Parte speciale, nella formazione o nell'attuazione delle decisioni. In tale evenienza è inviata immediata informazione all'OdV e, in ogni caso, è richiesta la successiva ratifica da parte del soggetto competente.

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi vigenti, ai valori e alle politiche aziendali e di Gruppo e alle regole contenute nel presente Modello.

In linea generale, il sistema di organizzazione aziendale deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

a) conoscibilità all'interno della Società (ed eventualmente anche nei confronti delle altre società del Gruppo);
b) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;
c) chiara descrizione delle linee di riporto.

Le procedure interne sono caratterizzate dai seguenti elementi:

A) ove possibile, massima separatezza possibile, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e lo conclude, e il soggetto che lo controlla;
B) traccia scritta di ciascun passaggio rilevante del processo;
C) adeguato livello di formalizzazione delle procedure organizzative;
D) evitare che i premi assegnati a soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna dipendano dalla realizzazione di target di performance sostanzialmente irraggiungibili.

Occorre rilevare che molte delle attività che potrebbero astrattamente condurre alla commissione di uno dei reati previsti dal D.lgs. 231/2001 sono in realtà presidiate e/o svolte, attraverso specifici contratti di servizio, da ciascuna delle competenti funzioni di Allianz ovvero di Arpa S.r.L..

Per tutte attività affidate in outsourcing ad Allianz (cfr. elenco presente nel precedente paragrafo 3.1 della Parte Generale) i contratti di servizio definiscono, tra gli altri; anche il potere di APP Broker di essere informata / monitorare la corretta esecuzione delle attività oggetto del servizio prestato.

Per lo svolgimento delle attività prestate dalla Capogruppo o da Società terze appartenenti al medesimo Gruppo, trovano pertanto applicazione le procedure/policy in uso presso Allianz S.p.A.

* * *

I contenuti della Parte Speciale trovano, raccordo e completamento nei presidi di controllo contenuti nel corpus regolamentare aziendale, nonché nelle policy/procedure della Capogruppo, in relazione alle attività da quest'ultima prestate nei confronti di APP Broker.

9.2. Il sistema di deleghe e procure

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei Reati (rintracciabilità ed evidenziabilità delle Attività Sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per "delega" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per "procura" il negozio giuridico unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti dei terzi. Ai titolari di una funzione aziendale, che necessitano per lo svolgimento dei loro incarichi di poteri di rappresentanza, viene conferita una "procura generale funzionale" di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la "delega".

I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei Reati sono i seguenti:

a) tutti coloro (compresi anche i dipendenti o gli organi sociali di altre società del Gruppo) che intrattengono per conto della società rapporti con la Pubblica Amministrazione devono essere dotati di delega formale in tal senso;

b) 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;

c) ciascuna delega deve definire in modo specifico ed inequivoco i poteri del delegato e il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;

d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;

e) il delegato deve disporre, ove necessario in relazione al potere conferito, di poteri di spesa adeguati alle funzioni conferitegli.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di una efficace prevenzione dei Reati, sono i seguenti:

- le procure generali descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione che fissi: l'estensione di poteri di rappresentanza ed i limiti di spesa numerici; ovvero i limiti assuntivi per categorie di rischio, richiamando comunque il rispetto dei vincoli posti dai processi di approvazione del *budget* e degli eventuali *extrabudget*, dai processi di determinazione dei poteri assuntivi, dai processi di monitoraggio delle Attività Sensibili da parte di funzioni diverse;
- la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;
- le procure speciali devono dettagliatamente stabilire l'ambito di operatività e i poteri del procuratore;
- le procure generali e speciali che consentono al soggetto che la riceve di rappresentare la Società nei confronti della Pubblica Amministrazione devono farne espressa menzione;
- 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 o estensione di nuove responsabilità e poteri, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, revoca, ecc.).

CAPITOLO 10 - REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (artt. 24 e 25 del Decreto)

10.1. Le fattispecie dei reati nei rapporti con la pubblica amministrazione.

Il presente capitolo 10 si riferisce ai reati realizzabili nell'ambito dei rapporti tra APP Broker e la Pubblica Amministrazione.

In particolare, gli articoli 24 e 25 contemplano diverse fattispecie di reati contro la pubblica amministrazione nonché alcuni reati contro il patrimonio commessi ai danni dello Stato o di altro ente pubblico.

Come noto, la legge 6 novembre 2012, n. 190, recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" ("Legge Anticorruzione"), ha riformato l'intero apparato normativo in materia di corruzione. Oltre a prevedere rigide regole comportamentali per i pubblici dipendenti e specifiche misure volte alla trasparenza dell'azione amministrativa, la legge ha apportato rilevanti modifiche in materia. Alle fattispecie già incluse nei c.d. "reati presupposto" della responsabilità ex Decreto 231 è andata ad aggiungersi quella della "induzione indebita a dare o promettere utilità" (art. 319-quater c.p.). Parallelamente, il legislatore è intervenuto sulla categoria dei reati societari di cui all'art. 25-ter del Decreto 231 introducendo la nuova figura del "reato di corruzione tra privati" (art. 2635 c.c.).

Si descrivono brevemente qui di seguito le singole fattispecie contemplate nel D.lgs. 231/2001 agli artt. 24 e 25 e ritenute applicabili, anche se in via prudenziale, data l'operatività di APP Broker.

- ***MALVERSAZIONE A DANNO DELLO STATO O DELL'UNIONE EUROPEA (ART. 316-BIS C.P.)***

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti, sovvenzioni o contributi da parte dello Stato italiano, di altro Ente pubblico o dell'Unione Europea, destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non si

proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

- ***INDEBITA PERCEZIONE DI EROGAZIONI IN DANNO DELLO STATO O DELL'UNIONE EUROPEA (ART. 316-TER C.P.)***

Tale ipotesi di reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere o mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità europea.

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato: essenzialmente laddove l'erogazione non sia l'effetto dell'induzione in errore dell'ente erogante.

- ***TRUFFA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640, COMMA 2 N. 1, C.P.)***

Tale ipotesi di reato – costituente un'ipotesi aggravata di truffa – incrimina la condotta di chi con artifici o raggiri induce taluno in errore procurandosi un ingiusto profitto con altrui danno, quando il fatto sia commesso a danno dello Stato o di altro ente pubblico.

Nella nozione di artifici (alterazione della realtà esteriore che si realizza o simulando l'inesistente o dissimulando l'esistente) o raggiri (consistenti essenzialmente in una menzogna qualificata corredata da ragionamenti e discorsi tali da farla recepire come veritiera) sono compresi anche la menzogna, o il silenzio maliziosamente serbato su alcune circostanze rilevanti ai fini della conclusione del contratto, quando abbiano determinato l'errore altrui, inducendo il soggetto ingannato a compiere un atto di disposizione patrimoniale dal quale sia conseguito un ingiusto profitto a favore dell'autore del reato, con altrui danno.

Ai fini della sussistenza della truffa ai danni dello Stato o di altro ente pubblico, è necessario che lo Stato (o altro ente pubblico) patisca il danno patrimonaile, mentre non è indispensabile che il soggetto ingannato rivesta una funzione pubblica (si pensi all'inganno ai danni di funzionario di banca che sia indotto a trasferire al truffatore denaro di un ente pubblico).

Il profitto può anche consistere in una mancata diminuzione patrimoniale o in altro vantaggio.

Nella nozione di ente pubblico rientra qualsiasi ente che persegua finalità pubbliche o svolga funzioni di preminente interesse pubblico.

Rileva precisare che la giurisprudenza ha spesso catalogato come enti pubblici anche i soggetti di diritto privato che siano concessionari di pubblici servizi nonché le società che siano partecipate a maggioranza da un ente pubblico.

- ***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 contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche da parte dello Stato, di enti pubblici o dell'Unione Europea.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere i finanziamenti pubblici.

- ***FRODE INFORMATICA IN DANNO DELLO STATO, DI ALTRO ENTE PUBBLICO (ART. 640-TER C.P.)***

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o intervenendo senza diritto su dati, informazioni o programmi in esso contenuti o ad esso pertinenti, procuri a sé o ad altri un ingiusto profitto con altrui danno. Anche la frode informatica, come la truffa, è fonte di responsabilità per l'ente se commessa ai danni dello Stato o di altro ente pubblico.

- ***CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE (ART.318 C.P.- CD. CORRUZIONE IMPROPRIA) E CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI D'UFFICIO (ART. 319 C.P.- CD. CORRUZIONE PROPRIA)***

La corruzione impropria, prevista dall'art.318 c.p., si configura nel caso in cui un pubblico ufficiale riceva, per sé o per un terzo, denaro o altra utilità o ne accetti la promessa per l'esercizio delle sue funzioni o dei suoi poteri.

La corruzione propria, prevista dall'art.319 c.p., si configura nel caso in cui un pubblico ufficiale riceva, per sé o per un terzo, denaro o altra utilità o ne accetti la promessa per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio o per compiere o aver compiuto un atto contrario ai doveri d'ufficio. L'art.320 c.p. estende l'applicabilità di entrambe le fattispecie agli incaricati di pubblico servizio.

Nel caso della corruzione impropria, l''attività del pubblico ufficiale (o dell'incaricato di pubblico servizio) è pienamente conforme all'interesse pubblico, e ciò che si intende punire è esclusivamente il cd. mercimonio della funzione pubblica.

Nel caso della corruzione propria il pubblico ufficiale accetta una retribuzione in cambio del compimento di un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per

garantire l'aggiudicazione di una gara), oppure dell'asservimento della pubblica funzione agli interessi del privato (es: offerta al pubblico ufficiale di denaro per assicurarsene i futuri favori).

Tale ipotesi di reato si differenzia dalla concussione, in quanto corrotto e corruttore operano su un piano paritario, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

- ***TRAFFICO DI INFLUENZE ILLECITE (ART. 346 BIS C.P.)***

Con la legge 9 gennaio 2019, n. 3, il legislatore italiano ha inserito anche l'illecito di cui all'art. 346-bis c.p. nel catalogo dei reati presupposto del Decreto. Si noti, peraltro, che con la medesima novella è stato abrogato, nel codice penale, il reato di millantato credito (art. 346 c.p.), facendo tuttavia "confluire" tale condotta illecita nel rinnovato testo dell'art. 346-bis c.p.

A seguito della riforma operata nel 2019, quindi, il reato di traffico di influenze illecite punisce chiunque, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di pubblico servizio – ovvero uno dei soggetto di cui all'art. 322-bis c.p. – indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di pubblico servizio – ovvero uno dei soggetti di cui all'art. 322-bis c.p. – oppure per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

- ***INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (ART.319-QUATER C.P.)***

Tale ipotesi di reato si configura nel caso in cui, un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o promettere indebitamente a lui o a un terzo denaro o altra utilità.

A differenza di quanto avviene per la concussione, in questo caso è punibile anche il soggetto che, per effetto delle pressioni subite, è indotto alla promessa o dazione di utilità. Si ritiene, infatti, che la minor intensità delle pressioni (di qui la differenza tra costrizione e induzione) consenta comunque al privato di non accedere alla richiesta.

- ***ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)***

Tale ipotesi di reato si configura quando il privato offre o promette denaro ad un pubblico ufficiale o ad un incaricato di pubblico servizio (per l'esercizio delle sue funzioni o per il compimento di un atto contrario ai suoi doveri), qualora l'offerta o la promessa non sia accettata; si configura inoltre quando il pubblico ufficiale o l'incaricato di pubblico servizio solleciti una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o per il compimento di un atto contrario ai suoi doveri.

Tale ipotesi di reato rappresenta quindi una "forma anticipata" del reato di corruzione. In particolare, il reato di istigazione alla corruzione si configura pertanto tutte le volte in cui, in presenza di un comportamento finalizzato alla commissione di un reato di corruzione , questa non si perfezioni in quanto una delle due parti non accetta l'offerta o non recepisca il sollecito proveniente dall'altra.

- ***CORRUZIONE IN ATTI GIUDIZIARI (ART. 319-TER)***

Tale ipotesi di reato si configura nel caso in cui i fatti di corruzione siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo; il destinatario dell'attività corruttiva può essere non solo un magistrato, ma anche un testimone, un cancelliere od un altro funzionario).

10.2 Criteri per la definizione di Ente della Pubblica Amministrazione, di pubblico ufficiale e di soggetto incaricato di un pubblico servizio

I reati ora esaminati sono reati contro la pubblica amministrazione, o reati commessi ai danni di enti pubblici. Inoltre, alcuni dei reati contro la pubblica amministrazione (i reati di concussione, corruzione e induzione indebita) presuppongono il coinvolgimento di un privato e di un soggetto che assuma la qualifica di pubblico ufficiale o incaricato di pubblico servizio.

Obiettivo del presente capitolo è, quindi, quello di indicare i criteri per l'individuazione della nozione di Ente della Pubblica Amministrazione nonché dei soggetti titolari di una delle qualifiche pubblicistiche rilevanti ai fini dei reati richiamati dalll'art.25 D.Lgs. 231/2001 (concussione, induzione indebita a dare o promettere utilità, corruzione).

10.2.1. Enti della Pubblica Amministrazione

Agli effetti della legge penale, viene comunemente considerato come "Ente della Pubblica Amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

A titolo esemplificativo, si possono indicare quali soggetti della Pubblica Amministrazione, i seguenti Enti, categorie di Enti o singole articolazioni di Enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Agenzia delle Entrate, Magistratura ordinaria e amministrativa);
- Regioni;
- Province;
- Autorità di Vigilanza (quali ad esempio IVASS, AGCM);
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;

- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAI, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano un pubblico servizio (ad esempio, la RAI);
- Fondazioni di previdenza ed assistenza.

Fermo restando la natura puramente esemplificativa di tale elenco, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di Reati nei rapporti con la Pubblica Amministrazione.

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

10.2.2. Pubblico Ufficiale

L'art. 357 c.p. definisce pubblici ufficiali "coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa", precisando che "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*".
Il Codice Penale prevede quindi 3 tipi di pubbliche funzioni: legislativa, giudiziaria ed amministrativa.
Le prime due (legislativa e giudiziaria) non sono definite espressamente dall'art. 357 c.p. perché presentano caratteristiche tipiche che consentono una loro immediata individuazione; infatti:

- la funzione legislativa è l'attività svolta dagli organi pubblici (Parlamento, Regioni e Governo) che, secondo la Costituzione italiana, hanno il potere di emanare atti aventi valore di legge;
- la funzione giudiziaria è l'attività svolta dagli organi giudiziari (civili, penali e amministrativi) e dai loro ausiliari (cancelliere, segretario, perito, interprete, etc.), per l'applicazione della legge al caso concreto.

La funzione amministrativa, così come definita dal comma secondo dell'art. 357 è un'attività che si caratterizza per il fatto di essere disciplinata da norme di diritto pubblico o da atti autoritativi della P.A. (e ciò la differenzia dalle attività di natura privatistica che sono disciplinate da strumenti di diritto privato, quali il contratto) e per la circostanza di essere accompagnata dalla titolarità di almeno uno dei seguenti tre poteri:

- potere di formare e manifestare la volontà della P.A. (ad es. sindaco o assessore di un comune, dirigenti di aziende pubbliche, etc.);
- potere autoritativo, che comporta l'esercizio di potestà attraverso le quali si esplica il rapporto di supremazia della P.A. nei confronti dei privati cittadini (ad esempio, gli appartenenti alle forze dell'ordine, i componenti delle commissioni di collaudo di lavori eseguiti per un ente pubblico, i funzionari degli organismi di vigilanza – Banca d'Italia, etc.);
- potere certificativo, vale a dire potere di redigere documentazione alla quale l'ordinamento giuridico attribuisce efficacia probatoria privilegiata (ad es. notai).

Per fornire infine un contributo pratico alla risoluzione di eventuali "casi dubbi", può essere utile ricordare che assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico - amministrativo dello Stato o di enti territoriali, ma anche tutti coloro che, in base allo statuto, nonché alle deleghe che esso consenta, ne formino legittimamente la volontà e/o la portino all'esterno in forza di un potere di rappresentanza.

Reati che possono essere commessi solo da o verso pubblici ufficiali

Art. 317	c.p.	Concussione
Art. 318	c.p.	Corruzione per l'esercizio di una funzione
Art. 319	c.p.	Corruzione per un atto contrario ai doveri d'ufficio
Art. 319 *ter*	c.p.	Corruzione in atti giudiziari
Art. 319 quater	c.p.	Induzione indebita a dare o promettere utilità
Art. 322	c.p.	Istigazione alla corruzione

10.2.3. Incaricato di un pubblico servizio

La definizione della categoria di "*soggetti incaricati di un pubblico servizio*" si rinviene all'art. 358 c.p. il quale recita che "*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio.*
Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, del pari alla "pubblica funzione", da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Esempi di incaricati di pubblico servizio sono: i dipendenti delle autorità di vigilanza che non concorrono a formare la volontà dell'autorità e che non hanno poteri autoritativi, i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, etc.

Reati che possono essere ascritti agli incaricati di pubblico servizi

Art. 318	c.p.	Corruzione per l'esercizio di una funzione
Art. 319	c.p.	Corruzione per un atto contrario ai doveri d'ufficio
Art. 319 *ter*	c.p.	Corruzione in atti giudiziari
Art. 319 quater	c.p.	Induzione indebita a dare o promettere utilità
Art. 322	c.p.	Istigazione alla corruzione

10.3 Attività Sensibili

Le principali Attività Sensibili, che APP Broker ha individuato al proprio interno come rilevanti per la presente famiglia di reati, sono le seguenti:

A) Rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza

L'Attività Sensibile in esame è relativa alla gestione dei rapporti con esponenti della Pubblica Amministrazione e delle Autorità di Vigilanza.

In particolare:

- Gestione dei rapporti con Funzionari competenti (INPS, INAIL, ASL, Direzione Provinciale del Lavoro ecc.) per l'osservanza degli obblighi previsti dalla normativa di riferimento, anche per il tramite di Capogruppo:
    - predisposizione delle denunce relative a costituzione, modifica ed estinzione del rapporto di lavoro;
    - elenchi del personale attivo, assunto e cessato presso l'INAIL;
    - controlli e verifiche circa il rispetto dei presupposti e delle condizioni previste dalla normativa vigente;
    - predisposizione ed esecuzione dei pagamenti verso lo Stato o altri Enti pubblici.
- Gestione dei rapporti, anche per il tramite di Capogruppo, con i Funzionari della Guardia di Finanza, dell'Agenzia delle Entrate e degli altri Enti competenti in materia fiscale e tributaria, nonché con l'Autorità di pubblica sicurezza, anche in occasione di verifiche, ispezioni ed accertamenti e gestione delle relative comunicazioni.
- Gestione dei rapporti e delle informazioni dirette alle Autorità Amministrative Indipendenti relativi allo svolgimento di attività regolate dalla normativa di riferimento, anche per il tramite di Capogruppo.

Si tratta in particolare della gestione dei rapporti con le Autorità di Vigilanza (ad esempio: IVASS, Autorità Garante per la Protezione dei dati personali), sia nell'attività ordinaria che in caso di verifiche, ispezioni ed accertamenti.

- Gestione degli adempimenti dei rapporti con i Funzionari degli Enti competenti in materia di adempimenti societari presso il Tribunale, la CCIAA e l'Ufficio del Registro, anche per il tramite di Capogruppo.
- Gestione dei rapporti, anche per il tramite di Capogruppo, con i funzionari pubblici per l'attuazione degli adempimenti richiesti dalla normativa vigente per le assunzioni agevolate (e.g. apprendistati professionalizzanti) e per le assunzioni di soggetti appartenenti a categorie protette, anche in occasione di verifiche ispettive.

B) Gestione e utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

L'Attività Sensibile in questione è rappresentata dell'attività di gestione e utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, con riferimento in particolare all'attività di trasmissione di dati su supporti informatici a pubbliche amministrazioni, enti pubblici o autorità (anche mediante accesso a sistemi informatici o telematici).

C) Selezione e assunzione del personale dipendente

L'Attività Sensibile in questione è stata inserita in via prudenziale e riguarda il processo di assunzione e di selezione dei dipendenti della Società.

L'attività rileva nella misura in cui il processo di selezione e assunzione del personale sia utilizzato come strumento indiretto per compiere atti di corruzione. In altre parole, qualora l'assunzione di una persona, ad esempio, legata al Soggetto Pubblico o comunque su segnalazione di quest'ultimo, anche per il tramite di una "costrizione" da parte dello stesso, sia finalizzata al riconoscimento di un indebito vantaggio in capo alla Società.

D) Gestione dei flussi monetari e finanziari

L'Attività Sensibile in questione riguarda la gestione dei flussi monetari e finanziari della Società, nel momento in cui la dazione/promessa di denaro a Soggetti Pubblici o a rappresentanti di Enti pubblici che gestiscono i rapporti per conto della P.A. posa essere finalizzata a trarre un ingiusto profitto per la Società.

E) Acquisto di beni, servizi e consulenze

L'Attività Sensibile in questione è stata inserita in via prudenziale e riguarda il processo di Acquisto di beni, servizi e consulenze, con particolare riguardo alla selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, riferita a soggetti pubblici (incluso soggetti privati collegati ovvero segnalati da Funzionario Pubblico), specialmente in relazione ad acquisti di natura immateriale, tra cui: consulenze direzionali, commerciali, amministrativo-legali e collaborazioni a progetto, pubblicità; sponsorizzazioni; spese di rappresentanza.

Rilevano a tal proposito tulle le fasi del processo di acquisto:

- Gestione della selezione del fornitore di servizi (inclusa la fase di qualifica / accreditamento del fornitore);
- Gestione della fase di definizione dell'acquisto di servizi (es. caratteristiche del servizio, etc.);
- Gestione del controllo sull'effettività del servizio acquistato (es. ricevimento dei beni, attestazione di avvenuta prestazione dei servizi, etc.);
- Gestione della contabilità e dei pagamenti (con riferimento, in particolare, alla fase di autorizzazione al pagamento).

10.4 Principi generali di comportamento

I seguenti principi di carattere generale si applicano a tutti i Destinatari del Modello nell'ambito dello svolgimento delle attività di pertinenza.

E’ fatto divieto di:

- promettere, offrire, corrispondere, direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per sé e/o per la Società, nemmeno assecondando il comportamento induttivo da parte del rappresentante della Pubblica Amministrazione;
- promettere, offrire, corrispondere omaggi o forme di ospitalità che eccedano le normali pratiche commerciali o di cortesia e, in ogni caso, tali da compromettere l’imparzialità e l’indipendenza di giudizio della controparte, nonché l’integrità e la reputazione di quest’ultima, nemmeno assecondando il comportamento induttivo da parte del Rappresentante della Pubblica Amministrazione. In caso di dubbio occorre darne tempestiva informazione al C.d.A. e comunicazione all'OdV. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche e tale documentazione deve essere portata a conoscenza dell'OdV;
- influenzare indebitamente i rapporti con la Pubblica Amministrazione e, in generale, con i terzi in relazione al business della Società;
- favorire nei processi di acquisto fornitori, consulenti o altri soggetti segnalati in cambio di vantaggi di qualsivoglia natura per sé e/o per la Società;
- favorire indebitamente un fornitore disapplicando le disposizioni contrattuali previste, accettando documentazione falsa o erronea, scambiando informazioni sulle offerte degli altri fornitori, approvando requisiti inesistenti, ricevendo servizi e forniture diverse da quelle contrattualmente previste;
- eseguire prestazioni e riconoscere compensi in favore delle Società di Service e dei Consulenti che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- accettare o ricevere omaggi o altri vantaggi, anche in denaro, volti a influenzare l’imparzialità e indipendenza del proprio giudizio;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;

- favorire, nei processi di assunzione e di selezione, dipendenti, collaboratori e consulenti, dietro specifica segnalazione, in cambio di favori, compensi e/o altri vantaggi per sé e/o per la Società;
- tenere una condotta ingannevole nei confronti della Pubblica Amministrazione, e dei terzi, inviando documenti falsi, rendicontando il falso, attestando requisiti inesistenti o fornendo garanzie non rispondenti al vero;
- presentare dichiarazioni non veritiere a Pubbliche Amministrazioni, nazionali e/o comunitarie, al fine di conseguire erogazioni pubbliche, quali ad esempio contributi, finanziamenti o altre agevolazioni;
- nel corso dello svolgimento di procedimenti giudiziari o indagini / ispezioni è fatto divieto di distruggere, alterare od occultare registrazioni, verbali, scritture contabili e qualsiasi tipo di documento o dato, dichiarare il falso ovvero persuadere altri a farlo, promettere o elargire omaggi, denaro o altre utilità ai funzionari preposti all'attività di accertamento o di controllo, in cambio di benefici per sé e/o per Società.

I rapporti con i Rappresentanti della Pubblica Amministrazione sono gestiti esclusivamente da persone munite di idonei poteri o da coloro che siano da queste formalmente delegati, e in ogni caso nel rispetto delle procedure della Società. In relazione ai dati forniti alla Pubblica Amministrazione, nell'ambito di ogni tipologia di rapporto, il referente di tale attività ha la specifica responsabilità di porre in essere tutti i controlli, diretti e indiretti, atti a garantire la correttezza, la veridicità e l'aggiornamento del dato o informazione che deve essere comunicato.

Per ciò che concerne il tema della sicurezza informatica si faccia riferimento al paragrafo successivo capitolo 11.

10.5 Principi specifici per le procedure

Ai fini dell'attuazione delle regole e divieti elencati al precedente paragrafo 10.4, devono rispettarsi i principi procedurali specifici qui di seguito descritti, oltre alle Regole e Principi Generali già contenuti nella Parte Generale del presente Modello.

A) Rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza

- alle visite ispettive (di qualsiasi tipologia, e.g. giudiziarie, tributarie e amministrative o di vigilanza) devono partecipare i soggetti a ciò espressamente delegati;
- l'OdV dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della persona di volta in volta interessata;
- di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali, che verranno conservati dall'OdV;
- le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di concessioni, autorizzazioni o licenze, devono contenere solo elementi assolutamente veritieri;
- fermo quanto disposto dal precedente punto, in ogni caso, deputato a intrattenere rapporti istituzionali con la Pubblica Amministrazione è il Presidente del C.d.A., ovvero il Responsabile operativo di APP Broker. Ciascun dipendente che intenda o abbia la necessità di intrattenere rapporti istituzionali con la P.A. dovrà preventivamente rivolgersi al Presidente del C.d.A., al fine di impostare il contatto ed il rapporto in maniera appropriata;
- alle eventuali Società di Service, Consulenti e Agenti che materialmente intrattengano rapporti con la Pubblica Amministrazione per conto di APP Broker, deve essere formalmente conferito potere in tal senso dalla stessa, con apposita clausola contrattuale. Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri elencati nel presente Modello.

La Società non partecipa a gare indette dalla Pubblica Amministrazione.

B) Gestione e utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

Per i principi procedurali si rimanda al successivo par. 11.4.

C) Selezione e assunzione del personale dipendente

1) La Società adotta una procedura che disciplini l'interazione tra i diversi uffici coinvolti nella selezione e assunzione del personale.

2) La selezione e assunzione del personale è ispirata a un criterio di trasparenza sulla base dei seguenti parametri:
   - professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
   - uguaglianza di trattamento tra i diversi candidati;
   - affidabilità rispetto al rischio di infiltrazione criminale.

3) La Società assicura che vengano prodotti prima dell'assunzione i seguenti documenti:
   - *curriculum vitae;*
   - casellario giudiziario;
   - certificato dei carichi pendenti, non anteriore a tre mesi.

4) La Società conserva la documentazione esibita in sede di assunzione anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

D) Gestione dei flussi monetari e finanziari

La Società attua specifici controlli procedurali e cura con particolare attenzione i flussi che non rientrano nei processi tipici dell'azienda e che sono quindi gestiti in modo estemporaneo e discrezionale. La finalità di detti controlli consiste nell'impedire la formazione di riserve occulte o

dazioni non giustificate di denaro o altre utilità che potrebbero essere il veicolo per la commissione di reati di corruzione.

- Nessun pagamento può essere effettuato in contanti;
- è stata adottata una policy interna, in tema di omaggi, che prevede il divieto di effettuare regali ed inviti salvo particolari casi;
- utlilizzo del c/c di APP BROKER (conto Allianz Bank).

Si precisa che la tesoreria è gestita in outsourcing da Allianz S.p.A. per conto di APP Broker.

E) Acquisto di beni, servizi e consulenze

1. Alle Società di Service e Consulenti che materialmente intrattengano rapporti con la P.A. per conto di APP Broker, deve essere formalmente conferito potere in tal senso dalla Società, con apposita clausola contrattuale. Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta;
2. i contratti tra APP Broker e le Società di Service e i Consulenti devono essere definiti per iscritto in tutte le loro condizioni e termini, e rispettare quanto indicato ai successivi punti;
3. i Consulenti devono essere scelti con metodi trasparenti e secondo specifica procedura aziendale che consenta di verificarne affidabilità e onorabilità, nel rispetto della quale la selezione deve avvenire tra i Consulenti "accreditati" dalla Società/Capogruppo nelle c.d. "*recommended list*"; le richieste di spesa eventualmente rivolte a soggetti "esterni" alla *recommended list* dovranno essere accompagnate da adeguata motivazione e pur sempre rispettando la procedura aziendale;
4. i contratti significativi (così come indicati nella procedura di cui la Società si dota) devono essere sottoposti al vaglio preventivo di contenuti e corrispettivi da parte della funzione e/o funzioni indicate nella suddetta procedura.
5. la Società inserisce nei contratti con i Professionisti una specifica clausola con la quale gli stessi dichiarano i) di essere a conoscenza del D.Lgs 231/01 e di non essere mai incorsi nella commissione di uno dei reati in discorso, ii) di prendere atto che la Societàha adottato il presente Modello, pubblicato sul sito web, iii) si impegna al rispetto della normativa alla base del Modello e

quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;

6. la Società inserisce nei contratti con Fornitori, Appaltatori e Broker una specifica clausola con la quale gli stessi dichiarano i) di essere a conoscenza del D.Lgs 231/01 e dichiara di non aver mai ricevuto condanne, anche non esecutive, per uno dei reati e degli illeciti amministrativi contemplati nel citato Decreto, ii) di prendere atto che la Società ha adottato il presente Modello, pubblicato sul sito web, iii) si impegna al rispetto della normativa alla base del Modello e quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;
7. la Società inserisce nei contratti infragruppo una specifica clausola con la quale si dichiara e si garantisce che, nell'espletamento delle attività previste dal contratto, non sarà posto in essere - obbligandosi anche per il fatto del proprio personale ai sensi dell'art. 1381 del Codice Civile - alcun atto od omissione da cui possa derivare una responsabilità ai sensi del citato D.lgs. n. 231/2001, impegnandosi ad agire nel pieno rispetto del proprio Modello di Organizzazione, Gestione e Controllo ex Decreto 231;
8. nei contratti con i Professionisti, i Fornitori, gli Appaltatori e i Broker, deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse).

Inoltre le procedure applicabili prevedono che per APP Broker e la Società di Service (per le parti di competenza):

- vi sia separazione di ruoli tra chi richiede l'acquisto e chi lo autorizza, istituendo una funzione ad hoc per la gestione di tutte le fasi dell'acquisto di beni e servizi;
- vi siano livelli autorizzativi diversi a seconda dell'importo dell'acquisto (sulla base delle procure rilasciate);
- sia verificata l'attendibilità e l'onorabilità dei fornitori aziendali;
- sia attuata una gara tra più fornitori per forniture superiori ad una soglia predeterminata ed indicata in apposita policy aziendale;
- sia assicurata la tracciabilità dell'intero processo di gestione degli acquisti.

CAPITOLO 11 – DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI (artt. 24 bis del Decreto)

11.1. Le fattispecie dei delitti informatici e di trattamento illecito di dati

Il presente capitolo 11 si riferisce ai delitti informatici e di trattamento illecito di dati.

Si descrivono brevemente qui di seguito le singole fattispecie contemplate nel D.lgs. 231/2001 all'art. 24 *bis* ritenute applicabili, anche se in via prudenziale, data l'operatività di APP Broker.

- ***FALSITÀ IN DOCUMENTI INFORMATICI (ART. 491 BIS C.P.)***

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti - ossia i delitti previsti dagli artt. 476 ss. c.p. – tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti cartacei.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, co. 1, *lett.* p, D.lgs. 82/2005).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato.

- ***ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615 TER C.P.)***

Tale reato si realizza quando un soggetto "*abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo*".

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma, secondo l'interpretazione prevalente, è il cd. "domicilio informatico" seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico.

La norma prevede due condotte distinte, l'"accesso" al sistema, ed il "mantenimento" nel sistema: l'accesso dev'essere abusivo e deve riguardare un sistema protetto da misure di sicurezza (nel concetto di misure di sicurezza è ricompresa una semplice password); il mantenimento nel sistema integra la fattispecie quando è effettuato contro la volontà del titolare del sistema.

Il reato sussiste quando la condotta di accesso o mantenimento nel sistema posta in essere dal soggetto agente, benché abilitato all'accesso, violi le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, onde delimitarne oggettivamente l'accesso, o quando l'agente ponga in essere operazioni di natura ontologicamente diversa da quelle per le quali l'accesso gli è consentito (Cass. Sez. Un. n.4694/2011).

Non rilevano, quindi, le finalità che soggettivamente hanno indotto l'ingresso nel sistema, mentre è rilevante la violazione delle prescrizioni di carattere organizzativo impartite per disciplinare le modalità di accesso agli strumenti informatici. Tali disposizioni, come precisato dalla giurisprudenza, possono consistere in disposizioni organizzative interne, prassi aziendali, clausole di contratti individuali di lavoro.

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di terzi (es. imprese concorrenti, etc.) o in uso ad altri dipendenti.

- ***DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615 QUATER C.P.)***

Tale reato si realizza quando un soggetto, "*al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo*".

Il Legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accesso abusivo a un sistema informatico. Per mezzo dell'art. 615 *quater* c.p., pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, *password* o schede informatiche (ad esempio, badge, carte di credito, bancomat e *smart card*).

Il delitto può risultare integrato, ad esempio, nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti.

- ***DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635 BIS C.P.)***

Tale fattispecie di reato si realizza quando un soggetto "distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui".

- ***DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635 QUATER C.P.)***

Questo reato di realizza quando un soggetto "*mediante le condotte di cui all'art. 635 bis (danneggiamento di dati, informazioni e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento*".

Quando l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto in esame e non quello di danneggiamento dei dati previsto dall'art. 635 *bis*.

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus).

11.2 Attività Sensibili

La principale Attività Sensibile rilevata da APP Broker nell'ambito dei delitti informatici e di trattamento illecito di dati, è la seguente:

A) Gestione ed utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

L'Attività Sensibile in esame fa riferimento ai seguenti ambiti:

- Gestione dei profili utente e del processo di autenticazione;
- Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio;
- Gestione e protezione della postazione di lavoro;
- Gestione degli accessi da e verso l'esterno;
- Gestione e protezione delle reti;
- Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD);
- Gestione della sicurezza fisica delle risorse informatiche.

B) Accesso e modifica dei dati contenuti nelle banche dati elettroniche, nei sistemi gestionali e di produzione

L'Attività Sensibile in esame fa riferimento all'accesso e modifica dei dati contenuti nella banche dati elettroniche, nei sistemi gestionali e di produzione, etc. da parte di soggetti con profilo di "System *Administrator*" e/o profilo di *superuser*.

11.3 Principi generali di comportamento

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano incaricati della gestione e manutenzione dei server, delle

banche dati, delle applicazioni e dei client, nonché a tutti coloro che abbiano avuto assegnate password e chiavi di accesso al sistema informativo aziendale:

- il personale si attiene rigorosamente alle policy aziendali in materia di gestione degli asset aziendali e, in particolare, della rete informatica della Società, in ogni caso facendone un uso appropriato rispetto alle proprie mansioni lavorative;
- il personale di astiene da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati aziendali e dei terzi;
- il personale si astiene da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale della Società o altrui (si tratti di soggetti pubblici o di soggetti privati);
- il personale non può utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa.

Nell'ambito dei suddetti comportamenti è fatto in particolare divieto di:

a) divulgare informazioni relative ai sistemi informatici aziendali;

b) utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta.

Al fine di limitare le rischiosità connesse alle tipologie di reato qui considerate, la Società:

a) fornisce, ai Destinatari, un'adeguata informazione circa il corretto utilizzo degli *user-id* e delle *password* per accedere ai principali sottosistemi informatici utilizzati presso la Società;

b) regolamenta, attraverso opportune *policy*, l'utilizzo dei sistemi informatici e l'accesso agli stessi da parte dei Destinatari sulla base delle finalità connesse agli impieghi da questi ultimi svolti;

c) effettua, per quanto possibile, nel rispetto della normativa sulla *privacy*, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali.

Valgono in particolare i seguenti principi generali:

- l'accesso alle informazioni che risiedono sui server aziendali, ivi inclusi i client, è limitato da strumenti di autenticazione;

- l'accesso alle applicazioni da parte del personale è garantito attraverso strumenti di autorizzazione;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (fisici e logici);
- il personale:
    - accede al sistema informativo aziendale unicamente attraverso i codici di identificazione assegnati, provvedendo alla modifica periodica;
    - assicura l'integrità e la non alterabilità dei dati, delle informazioni e dei programmi informatici che costituiscono lo strumento di svolgimento dell'attività lavorativa nonché dell'intero patrimonio informatico e telematico della Società;
    - contribuisce alla promozione di un adeguato livello di salvaguardia del patrimonio informatico e telematico altrui, sia esso privato o pubblico, conformemente alle modalità di controllo attivate dalla Società.

11.4 Principi specifici per le procedure

La Società applica le policy per la sicurezza informatica della Capogruppo e della Società di Service per le attività riconducibili a tale ambito, all'interno delle quali vengono disciplinate le modalità di gestione, utilizzo e protezione delle risorse informatiche della stessa, in linea con la normativa vigente applicabile (e.g. Codice in materia di protezione dei dati personali).

Relativamente alle Attività Sensibili identificate al precedente paragrafo 11.2 si applicano i seguenti principi.

A) Gestione ed utilizzo dell'infrast ruttura tecnologica e dei sistemi informativi e telematici aziendali

Ai Destinatari è fatto divieto di:

- modificare in qualsiasi modo la configurazione delle postazioni di lavoro fisse o mobili assegnate dalla Società;

- installare o utilizzare strumenti *software* e/o *hardware* che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (es. sistemi per individuare le *password*, decifrare i file criptati, ecc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, o di terzi con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale di clienti o di terzi, comprensivo di dati, archivi e programmi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali;
- divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi ed alla rete aziendale o di terzi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terzi per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- manipolare i dati presenti sui propri sistemi come risultato dei processi di *business*;
- danneggiare, distruggere o manomettere documenti informatici aventi efficacia probatoria, registrati presso enti pubblici (es. polizia, uffici giudiziari, ecc.), e relativi a procedimenti o indagini giudiziarie in cui la Società sia coinvolta a qualunque titolo.

La Società a sua volta pone in essere i seguenti adempimenti:

- informare adeguatamente i Destinatari dell'importanza di mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
- informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici;
- informare i Destinatari della necessità di spegnere (*log off*) i propri sistemi informatici al termine della giornata lavorativa;
- impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- fornire un accesso da e verso l'esterno (connessione alla rete Internet) esclusivamente ai sistemi informatici dei Destinatari che ne abbiano necessità ai fini lavorativi;

- dotare la stanza dei *server* di porta con chiusura a chiave;
- proteggere per quanto possibile ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi *hardware* in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- fornire ogni sistema informatico di adeguato *software firewall* e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti;
- qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante router dotati di antenna WiFi), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i router della stessa e compiere illeciti ascrivibili ai dipendenti della Società;
- limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei destinatari (ad esempio, oltre allo *username* ed alla *password*, fornire ai soggetti che abbiano necessità di collegarsi alla rete societaria dall'esterno un "*token*" - una chiavetta – in grado di generare password casuali necessarie per l'accesso).

Sono oggetto di reportistica periodica nei confronti dell'OdV:

- descrizione dei sistemi informatici/ software in uso presso la compagnia per trasmettere flussi informativi e controlli effettuati sul funzionamento degli stessi;
- relazione sulle procedure di utilizzo dei sistemi informativi aziendali e attività di potenziamento e miglioramento degli stessi.

B) Accesso e modifica dei dati contenuti nelle banche dati elettroniche, nei sistemi gestionali e di produzione

Con riferimento alla presente Attività Sensibile trovano applicazione i principi procedurali enunciati con riferimento alla precedente attività sensibile (cfr. precedente punto A).

CAPITOLO 12 – DELITTI DI CRIMINALITÀ ORGANIZZATA, ANCHE DI CARATTERE TRANSNAZIONALE (art. 24 ter del Decreto)

12.1. Le fattispecie dei delitti di criminalità organizzata

Il presente capitolo si riferisce ai reati di criminalità organizzata. Si indicano qui di seguito le singole fattispecie contemplate nel D.lgs. 231/2001 all'art. 24 ter ritenute applicabili, anche se in via prudenziale, data l'operatività di APP Broker:

- ***ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.)***

La condotta sanzionata dall'art. 416 c.p. è integrata mediante la costituzione e la conservazione di un vincolo associativo continuativo, tra tre o più persone, allo scopo di commettere una serie indeterminata di delitti, con la predisposizione di mezzi necessari per la realizzazione del programma criminoso.

Il reato associativo è caratterizzato, pertanto, dai seguenti elementi fondamentali:

- *stabilità e permanenza*: il vincolo associativo deve essere tendenzialmente stabile e destinato a durare anche oltre la realizzazione dei delitti concretamente programmati;
- *indeterminatezza del programma criminoso*: l'associazione a delinquere non si configura se i partecipanti si associano al fine di compiere un solo reato; lo scopo dell'associazione deve essere quello di commettere più delitti, anche della stessa specie (in tal caso l'indeterminatezza del programma criminoso ha riguardo solo all'entità numerica);
- *esistenza di una struttura organizzativa*: l'associazione deve prevedere un'organizzazione di mezzi e di persone che, seppure in forma rudimentale, siano adeguati a realizzare il programma criminoso e a mettere in pericolo l'ordine pubblico.

In particolare, sono puniti coloro che promuovono, costituiscono o organizzano l'associazione, oltre a coloro che regolano l'attività collettiva da una posizione di superiorità o supremazia gerarchica, definiti dal testo legislativo come "capi".

Sono puniti altresì con una pena inferiore tutti coloro che partecipano all'associazione.

Il reato in questione assume rilevanza ai fini della responsabilità amministrativa degli enti anche se commesso a livello "transnazionale" ai sensi dell'art. 10 della Legge 16 marzo 2006, n. 146 (legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale).

A tal riguardo giova sottolineare che ai sensi dell'art. 3 della suddetta legge 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, 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.

Come emerge dalla descrizione del reato in esame, attraverso lo strumento del reato associativo potrebbero essere commessi altri reati, siano essi espressamente previsti dal Decreto 231 oppure non rientranti tra le fattispecie delittuose che autonomamente comportano la responsabilità amministrativa dell'ente.

Le tipologie di reati previsti espressamente dal Decreto 231 sono state analizzate ed approfondite nelle relative Parti Speciali (cui occorre rinviare), indipendentemente dalla circostanza che la loro esecuzione avvenga in forma associativa o meno.

Quanto invece ai reati non previsti espressamente dal Decreto 231,al momento la giurisprudenza pare escludere, sia pure ai fini dell'individuazione del profitto confiscabile, che agli stessi si possa dare rilevanza nella prospettiva di una loro imputazione quali delitti-scopo del reato associativo, in base al rilievo che in tal modo l'art.416 c.p. si trasformerebbe in una disposizione "aperta", in violazione del principio di tassatività del sistema sanzionatorio contemplato dal D.Lgs.n.231/2001 (Cass. pen. sez.VI, n.3635/13). Ad oggi non risultano sentenze successive di segno diverso

12.2 Attività Sensibili

Di seguito sono descritte le principali Attività Sensibili che APP Broker ha individuato al proprio interno:

A) Selezione e assunzione del personale dipendente

L'Attività Sensibile in questione riguarda il processo di assunzione e di selezione dei dipendenti della Società, anche con riferimento ad eventuale nuovo personale assunto in agenzia nel corso della gestione interinale della stessa.

B) Selezione delle controparti contrattuali

L'Attività Sensibile in questione è stata inserita in via prudenziale e riguarda il processo di Selezione delle controparti contrattuali, con particolare riferimento ai Consulenti, ai Fornitori ed ai Partner.

Tale attività è rilevante in considerazione del fatto che l'instaurazione di rapporti con le stesse potrebbe rappresentare un fondamentale presupposto fattuale per la successiva commissione di reati associativi.

12.3 Principi generali di comportamento

I seguenti principi di carattere generale si applicano a tutti i Destinatari del presente Modello compresi – in via diretta – i Consulenti, le Società di Service e i Partner in forza di apposite clausole contrattuali.

E' ovviamente fatto divieto in via generale di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24 ter del D.Lgs. 231/2001).

Nell'ambito delle attività sensibili è fatto divieto in particolare di:

a) procedere all'assunzione di personale in azienda (dipendenti, collaboratori a progetto, stagisti ecc.) senza aver prima constatato la sussistenza di requisiti di onorabilità e affidabilità;

b) instaurare rapporti con soggetti terzi - persone fisiche o giuridiche, italiane o straniere - senza aver rispettato criteri e metodologie di selezione previsti dalle procedure aziendali che consentano di accertarne onorabilità e affidabilità;
c) intestare conti correnti a prestanomi, aprire e gestire fondi extracontabili e intestare beni fittiziamente.

Devono altresì essere rispettati i seguenti obblighi:
a) il processo di selezione del personale aziendale (dipendenti, collaboratori a progetto, stagisti ecc.) è costantemente regolato dal principio della segregazione dei ruoli;
b) il processo di selezione delle controparti contrattuali è costantemente regolato dal principio della segregazione dei ruoli;
c) la persistenza in capo a controparti contrattuali dei requisiti richiesti in fase di selezione è sottoposta a periodici controlli;
d) la Società monitora la perdurante efficacia delle procedure adottate per prevenire rischiosità connesse alle Attività Sensibili di cui al capitolo 12.2.

12.4 Principi specifici per le procedure

Relativamente alle Attività Sensibili identificate al precedente paragrafo 12.2 si applicano i seguenti principi:

A) Selezione e assunzione del personale dipendente

1) La Società adotta una procedura che disciplini l'interazione tra i diversi uffici coinvolti nella selezione e assunzione del personale, sia interni, sia della Capogruppo.

2) La selezione e assunzione del personale è ispirata a un criterio di trasparenza sulla base dei seguenti parametri:

- professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;

- uguaglianza di trattamento tra i diversi candidati;
- affidabilità rispetto al rischio di infiltrazione criminale.

3) La Società assicura che vengano prodotti prima dell'assunzione i seguenti documenti:

- curriculum vitae;
- casellario giudiziario;
- certificato dei carichi pendenti, non anteriore a tre mesi.

4) La Società conserva la documentazione esibita in sede di assunzione anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

5) La Società provvede ad effettuare periodici controlli circa il puntuale rispetto in fase di selezione del personale dei principi sopra elencati.

B) Selezione delle controparti contrattuali

1. La Società garantisce che il processo di selezione avvenga nel rispetto dei principi di trasparenza, onorabilità, pari opportunità di accesso, professionalità, affidabilità ed economicità; in particolare:

Fornitori e Consulenti:

- la Società adotta una procedura aziendale per la gestione dei rapporti con i medesimi, la quale preveda una verifica preliminare del possesso da parte degli stessi dei necessari requisiti di affidabilità e onorabilità;
- la procedura di cui al precedente punto 1) disciplina altresì il processo di acquisto del bene o la fornitura dell'attività consulenziale, indicando le unità coinvolte, le modalità di richiesta di autorizzazione alla spesa e di effettuazione dei relativi pagamenti, nonché di contabilizzazione dell'importo;
- con particolare riferimento ai professionisti, la Società richiede esibizione di documentazione comprovante l'iscrizione all'ordine professionale;

Accordi di collaborazione con Agenti e Broker:

- gli eventuali nuovi Agenti e Broker, con i quali instaurare accordi di collaborazione, vengono selezionati dalla Società, con il supporto della della Capogruppo, con metodi trasparenti e attraverso apposite *check list* all'uopo formulate dalla Società che consentono una verifica preliminare dell'affidabilità e dell'onorabilità degli stessi.

2. La Società verifica periodicamente il possesso dei requisiti dell'affidabilità e onorabilità in capo a Fornitori, Consulenti, Agenti, Broker e Partner.

3. La Società inserisce nei contratti con i Professionisti una specifica clausola con la quale gli stessi dichiarano i) di essere a conoscenza del D.Lgs 231/01 e di non essere mai incorsi nella commissione di uno dei reati in discorso, ii) di prendere atto che la Società ha adottato il presente Modello, pubblicato sul sito web, iii) si impegna al rispetto della normativa alla base del Modello e quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;

4. La Società inserisce nei contratti con Fornitori, Appaltatori e Broker una specifica clausola con la quale gli stessi dichiarano i) di essere a conoscenza del D.Lgs 231/01 e dichiara di non aver mai ricevuto condanne, anche non esecutive, per uno dei reati e degli illeciti amministrativi contemplati nel ciato Decreto, ii) di prendere atto che la Società ha adottato il presente Modello, pubblicato sul sito web, iii) si impegna al rispetto della normativa alla base del Modello e quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;

5. La Società inserisce nei contratti infragurppo una specifica clausola con la quale si dichiara e si garantisce che, nell'espletamento delle attività previste dal contratto, non sarà posto in essere - obbligandosi anche per il fatto del proprio personale ai sensi dell'art. 1381 del Codice Civile - alcun atto od omissione da cui possa derivare una responsabilità ai sensi del citato D.lgs. n. 231/2001, impegnandosi ad agire nel pieno rispetto del proprio Modello di Organizzazione, Gestione e Controllo ex Decreto 231;

6. Nei contratti con i Professionisti, i Fornitori, gli Appaltatori e i Broker, deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse);

7. Nei contratti con Fornitori, Consulenti e Sub-Agenti la Società inserisce altresì la specifica clausola anti-corruption.

CAPITOLO 13 – REATI SOCIETARI (Art. 25 ter del Decreto)

13.1. Le fattispecie dei reati societari

Il presente capitolo 13 si riferisce ai reati societari. Si descrivono brevemente qui di seguito le singole fattispecie contemplate nel D.lgs. 231/2001 all'art. 25 *ter* ritenute applicabili, anche se in via prudenziale, data l'operatività di APP Broker.

- ***FALSE COMUNICAZIONI SOCIALI (ARTT. 2621 E 2622 C.C.)***

L'art. 2621 c.c. si applica agli amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci, i quali, al fine di conseguire per sè o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico, espongono fatti materiali rilevanti non rispondenti al vero, ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo idoneo ad indurre altri in errore.

Si precisa che:

- le informazioni false o omesse devono essere tali da alterare la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;

- la stessa pena si applica se le falsità o le omissioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

- Il reato previsto dall'articolo 2622 c.c. si applica, invece, alle società emittenti strumenti finanziari ammessi alla negoziazione in Italia o in un paese dell'Unione Europa o alle società a queste equiparate, vale a dire:

1) le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;

2) le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano;

3) le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;

4) le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

L'art. 2622 c.c. attribuisce rilevanza anche a comunicazioni non previste dalla legge e non richiede che i fatti materiali non rispondenti al vero siano anche rilevanti.

- ***IMPEDITO CONTROLLO (ART. 2625 C.C.)***

Il reato di impedito controllo è integrato dal fatto degli amministratori che impediscono od ostacolano, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali, cagionando un danno ai soci.

- ***FORMAZIONE FITTIZIA DEL CAPITALE (ART. 2632 C.C.)***

L'art.2632 c.c. si applica agli amministratori e ai soci conferenti che, anche in parte, formano o aumentano fittiziamente il capitale della società mediante: attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale; sottoscrizione reciproca di azioni o quote; sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti ovvero del patrimonio della società nel caso di trasformazione.

- ***INDEBITA RESTITUZIONE DEI CONFERIMENTI (ART. 2626 C.C.)***

La "condotta tipica" prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

Si precisa che soggetti attivi sono gli amministratori.

La fattispecie in esame, così come quella successiva prevista dall'art. 2627, sanziona una condotta idonea a determinare un pregiudizio per la società, risolvendosi in una forma di aggressione al capitale sociale, a vantaggio dei soci.

Sotto un profilo astratto, pare invero difficile che il reato in esame possa essere commesso dagli amministratori nell'interesse o a vantaggio della società, implicando in tal modo una responsabilità dell'ente. Più delicato si presenta il problema in relazione ai rapporti intragruppo, essendo possibile che una società, avendo urgente bisogno di disponibilità finanziarie, si faccia indebitamente restituire i conferimenti effettuati a favore di un'altra società del gruppo. In tale ipotesi, in considerazione della posizione assunta dalla prevalente giurisprudenza che disconosce l'autonomia del gruppo societario inteso come concetto unitario, è ben possibile che, sussistendone tutti i presupposti, possa configurarsi una responsabilità dell'ente per il reato di indebita restituzione dei conferimenti commesso dai suoi amministratori.

- ***ILLEGALE RIPARTIZIONE DEGLI UTILI O DELLE RISERVE (ART. 2627 C.C.)***

Tale condotta criminosa consiste: nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva; ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

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

- ***ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (ART. 2628 C.C.)***

Questo reato si perfeziona con l'acquisto o la sottoscrizione, al di fuori dei casi consentiti dalla legge, di azioni o quote sociali della società, ovvero emesse dalla Società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

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

- ***OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (ART. 2629 C.C.)***

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altre società o scissioni, che cagionino danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

- ***CORRUZIONE TRA PRIVATI (ART. 2635 C.C.)***

In seguito alla pubblicazione in Gazzetta Ufficiale del Decreto legislativo 15 marzo 2017, n. 38, recante "Attuazione della decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003, relativa alla lotta contro la corruzione nel settore privato" (G.U. n. 75 del 30 marzo 2017), l'articolo 2635 c.c. è stato oggetto di una profonda rivisitazione. Nello specifico, la disposizione ora punisce, salvo che il fatto costituisca reato più grave, «gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà». Ai sensi del medesimo comma, poi, la stessa pena si applica se il fatto è commesso da chi, nell'ambito organizzativo della società o dell'ente privato, «esercita funzioni direttive diverse» rispetto a quelle indicate. Inoltre, l'art. 2635, co. 2, c.c. punisce – con una pena inferiore – gli stessi fatti se commessi «da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati dal primo comma».

A rilevare ai sensi dell'art. 25-ter, co 1, lett. s-bis) del D.lgs. 231/2001 è, invece, il terzo comma dell'art. 2635 c.c. che punisce chi, anche per interposta persona, «offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma».

Quindi, con riferimento a questa fattispecie di reato, una eventuale responsabilità può sorgere in capo all'ente solo nel caso in cui un soggetto apicale o un soggetto sottoposto alla vigilanza dello stesso prometta denaro o altra utilità ad un esponente di un altro ente al fine di avvantaggiare il proprio e

non, invece, nel caso in cui riceva o accetti la promessa. In breve, è prevista la responsabilità amministrativa dell'ente di appartenenza del corruttore, non dell'ente di appartenenza del corrotto.

La norma prevede un regime di procedibilità diversificato (d'ufficio o a querela) a seconda che dal fatto derivi o meno una distorsione della concorrenza nella acquisizione di beni o servizi.

- ***ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI (ART. 2635-BIS C.C.)***

L'introduzione del nuovo articolo 2635-bis del Codice civile riguarda invece la "Istigazione alla corruzione tra privati", fattispecie volta a punire chi mira a corrompere le figure dirigenziali che operano all'interno di società private.

In particolare, la condotta rilevante ai sensi dell'art. 25-ter, co. 1, lett. s-bis) del Decreto si realizza attraverso l'offerta o promessa di denaro o altra utilità non dovuti ai soggetti apicali o aventi funzioni direttive in società o enti privati, affinché questi ultimi compiano od omettano atti in violazione degli obblighi inerenti all'ufficio o degli obblighi di fedeltà, quando l'offerta o la promessa non sia accettata (art. 2635-bis, co. 1, c.c.) .

- ***OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA (ART. 2638 C.C.)***

L'art.2638 c.c. si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari e ai sindaci di società o enti e altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali pongono in essere una delle seguenti condotte

- espongono nelle comunicazioni alle Autorità di vigilanza previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, o su beni posseduti o amministrati dalla società per conto di terzi;

- allo stesso fine, occultano in tutto o in parte, con altri mezzi fraudolenti, fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, o beni posseduti o amministrati dalla società per conto di terzi;

- ostacolano le funzioni delle Autorità di vigilanza in qualsiasi forma, anche mediante omissione delle comunicazioni dovute.

In tale contesto gli ambiti di attività in relazione ai quali si prospetta un dovere di collaborazione con l'Autorità di vigilanza possono essere molteplici, pertanto, si impone una particolare attenzione ad improntare i rapporti con le Autorità di vigilanza a criteri di correttezza, trasparenza e collaborazione, evitando comportamenti che possano in qualsiasi modo considerarsi di ostacolo all'attività che tali autorità sono chiamate a svolgere.

- ***AGGIOTAGGIO (ART. 2737 C.C.)***

La fattispecie – richiamata nell'art.25-ter D.Lgs.n.231/2001 sui Reati societari – incrimina la condotta di chiunque diffonda notizie false ovvero ponga in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

La fattispecie in esame – nel tutelare il regolare funzionamento del mercato (aggiotaggio cd. societario) riguarda i soli strumenti finanziari non quotati.
La fattispecie tutela inoltre la stabilità del sistema bancario (aggiotaggio cd. bancario).

13.2 Attività Sensibili

Le principali Attività Sensibili, che APP Broker ha individuato al proprio interno come rilevanti per la presente famiglia di reati, sono le seguenti.

A) Gestione dei rapporti con l'Autorità di Vigilanza/ Organi di Controllo

L'Attività Sensibile in esame riguarda i rapporti con l'Autorità di Vigilanza e/o con gli Organi di Controllo in merito ai seguenti aspetti:

- Gestione dei rapporti e delle informazioni dirette alle Autorità Amministrative Indipendenti (ad esempio Autorità Garante per la Protezione dei dati personali), anche in occasione di verifiche, ispezioni ed accertamenti.
- Gestione dei rapporti con gli Organi di Controllo relativamente alle verifiche sulla gestione amministrativa/contabile e sul Bilancio d'Esercizio e con il Socio nelle attività di verifica della gestione aziendale.
- Tenuta delle scritture contabili e dei Libri Sociali.

B) Redazione e conservazione dei documenti contabili e adempimenti informativi / societari

L'Attività Sensibile in esame riguarda i seguenti aspetti:

- Coordinamento e gestione della contabilità generale, con particolare riferimento alle attività di:
  - rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi, finanziari ed economici;
  - corretta tenuta dei rapporti amministrativi con i terzi (e.g. clienti, fornitori);
  - gestione amministrativa e contabile dei fornitori, dei cespiti, e dei clienti (anche con riferimento ad operazioni inter-company);
  - accertamenti di tutti gli altri fatti amministrativi in corso d'anno (e.g. costi del personale, penalità contrattuali, finanziamenti passivi e relativi interessi, ecc.);
  - verifica dati provenienti dai sistemi alimentanti.
- Raccolta, aggregazione e valutazione dei dati contabili necessari per la predisposizione della bozza di Bilancio Civilistico della Società, nonché delle relazioni allegate ai prospetti economico-patrimoniali di bilancio da sottoporre alla delibera del Consiglio di Amministrazione.
- Collaborazione e supporto all'Organo Amministrativo per la predisposizione di situazioni patrimoniali funzionali alla realizzazione di:
  - Operazioni straordinarie;

- Operazioni di aumento/riduzione del capitale sociale;
- Altre operazioni su quote sociali o della Società.

- Collaborazione e supporto all'Organo Amministrativo nello svolgimento delle attività di ripartizione degli utili di esercizio, delle riserve e restituzione dei conferimenti.
- Collaborazione e supporto all'Organo Amministrativo per l'effettuazione delle operazioni di incremento/riduzione del capitale sociale o di altre operazioni su azioni o quote sociali o della società controllante.

*Con particolare riferimento al reato di **corruzione tra privati e istigazione alla corruzione tra privati**, sono state individuate le seguenti Attività Sensibili.*

C) Gestione dei rapporti di alto profilo con soggetti privati

L'Attività Sensibile in esame riguarda la gestione dei rapporti di alto profilo con

- clientela privata potenziale, nell'ambito dell'attività di collocamento di prodotti assicurativi da parte dei soggetti che operano per conto della Società, sia nei casi di rapporto diretto con il cliente da parte della Società;
- con altri intermediari assicurativi (agenti e broker), con particolare rifermento alla:
  - definizione dei mandati di collaborazione con altri broker o agenzie;
  - svolgimento delle attività di brokeraggio.

D) Acquisto di beni, servizi e consulenze

L'Attività sensibile in oggetto è stata inserita in via prudenziale.

Selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, riferita a soggetti privati, specialmente in relazione ad acquisti di natura immateriale, tra cui: consulenze direzionali, commerciali, amministrativo-legali e collaborazioni a progetto; pubblicità; sponsorizzazioni; spese di rappresentanza. Ed in particolare con riferimento alle attività di:

- gestione della selezione del fornitore di servizi (inclusa processo di qualifica / accreditamento del fornitore);
- gestione della fase di definizione dell'acquisto di servizi;
- gestione del controllo sull'effettività del servizio acquistato (es. ricevimento dei beni /attestazione di avvenuta prestazione dei servizi);
- gestione della contabilità e dei pagamenti (e in particolare con riferimento alla fase di autorizzazione al pagamento).

E) Gestione dei contenziosi

L'Attività Sensibile in esame riguarda la 'Gestione dei rapporti con parti terze per la definizione di:

- situazioni pre-contenziose;
- contenziosi intrapresi nei confronti della Società;
- accordi transattivi/conciliazioni.

F) Selezione e assunzione del personale dipendente

L'Attività Sensibile in questione è stata inserita in via prudenziale e riguarda il processo di assunzione e di selezione dei dipendenti della Società.

G) Gestione dei flussi monetari e finanziari

L'Attività Sensibile in questione riguarda la gestione dei flussi monetari e finanziari della Società.

13.3 Principi generali di comportamento

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività “sensibili” rispetto ai reati societari di cui all’art. 25 *ter* del D.Lgs. 231/2001.

È previsto l'espresso divieto a carico dei Destinatari (per quanto coinvolti nelle Attività Sensibili) di commettere o di concorrere alla realizzazione di azioni od omissioni tali da concretare, direttamente od indirettamente, i reati societari contemplati dal Decreto.

In via generale, ai Destinatari è richiesto di:

- 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 dei documenti contabili e delle comunicazioni sociali, ovvero alla formazione del bilancio, al fine di fornire al Socio e al pubblico un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale prevista dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- osservare le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- garantire che tutte le operazioni di rilevazione e registrazione delle attività di impresa siano effettuate con correttezza e nel rispetto dei principi di veridicità e completezza.

In tale prospettiva, è vietato:

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi, che non rappresentino in modo veritiero la situazione economica, patrimoniale e finanziaria della Società;

b) omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;

c) esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie di APP Broker;

d) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità di vigilanza;

e) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;

f) porre in essere comportamenti che impediscano, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, ovvero ostacolino lo svolgimento dell'attività di controllo e di revisione da parti del socio;

g) occultare informazioni richieste dal Socio, ovvero trasmettere a questi ultimi informazioni non corrispondenti al vero;

h) omettere la trasmissione di informazioni e/o l'esibizione della documentazione richiesta dal Socio;

i) alterare i Libri Sociali, le informazioni e la documentazione societaria e amministrativo-contabile attraverso artifici idonei a impedire o a ostacolare il controllo da parte dei soggetti titolati;

j) omettere l'esibizione dei Libri Sociali al Socio che ne faccia richiesta;

k) acquistare o sottoscrivere quote proprie della Società;

l) procedere ad aumento fittizio del capitale sociale, attribuendo quote per un valore inferiore al loro valore nominale;

m) restituire, anche simulatamente, i conferimenti al socio o liberarlo dall'obbligo di eseguirli, fatte salve ovviamente le ipotesi di legittima riduzione del capitale sociale;

n) ripartire utili o acconti su utili non effettivamente conseguiti, o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite;

o) effettuare riduzioni del capitale sociale o fusioni con altre società o scissioni in violazione delle norme di legge, con ciò cagionando un danno ai creditori;

p) formare o aumentare fittiziamente il capitale sociale mediante attribuzioni di azioni per somma inferiore al loro valore nominale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio sociale in caso di trasformazione.

* * *

Con particolare riferimento al reato di ***corruzione tra privati e istigazione alla corruzione tra privati***, devono essere rispettati i principi generali di comportamento qui di seguito descritti.

APP Broker rifugge il ricorso a qualunque forma di pratica corruttiva per raggiungere i propri obiettivi economici.

In particolare, è fatto divieto, in favore di un amministratore, direttore generale, dirigente preposto, sindaco o qualunque soggetto appartenente ad un ente terzo con il quale APP Broker intrattenga rapporti commerciali ed operativi e loro sottoposti, di:

- promettere o effettuare erogazioni in denaro;
- promettere, offrire o corrispondere omaggi che eccedano le normali pratiche commerciali o di cortesia e, in ogni caso, tali da compromettere l'imparzialità e l'indipendenza di giudizio della controparte;
- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti in quanto indicati dai soggetti di cui sopra;
- prendere in considerazione o proporre un'opportunità di impiego a favore dei terzi di cui sopra;
- promettere o concedere vantaggi di qualsiasi natura, con l'obiettivo di procurare un vantaggio indebito per APP Broker.

Ogni operazione deve essere registrata e documentata, al fine di consentirne adeguata tracciabilità.

Nell'ambito delle relazioni con terze parti di natura privata valgono inoltre i presidi di controllo in vigore a tutela dei rapporti con controparti pubbliche, nonché le procedure / linee guida di riferimento in relazione alla segregazione dei ruoli / tracciabilità delle attività / iter autorizzativo e poteri di spesa (cfr. successivo paragrafo 13.4).

13.4 Principi specifici per le procedure

Ai fini dell'attuazione delle regole elencate al precedente paragrafo 13.3, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali specifici qui di seguito descritti.

A) Gestione dei rapporti con l'Autorità di Vigilanza/ Organi di Controllo

- nel corso dell'attività ispettiva, deve essere prestata da parte delle funzioni e delle articolazioni organizzative ispezionate la massima collaborazione all'espletamento degli accertamenti. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati dell'ispezione ritengano necessario acquisire;

- alle ispezioni devono partecipare i soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione deve essere redatto e conservato apposito verbale. Nel caso il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del Responsabile operativo di APP Broker.

B) Redazione e conservazione dei documenti contabili e adempimenti informativi / societari

APP Broker adotta procedure interne che consentono**:**

- di determinare con chiarezza e completezza i dati e le informazioni contabili e finanziarie che ciascuna funzione interna deve produrre ai fini di una successiva elaborazione, ad opera di

Società di Service, delle comunicazioni contabili (es. bilancio mensile) da inoltrare alla Capogruppo;

- la predisposizione di un adeguato sistema di controllo teso a garantire una ragionevole certezza sulla veridicità e completezza dei suddetti dati e comunicazioni.

Con particolare riferimento alla predisposizione del Bilancio, relazioni allegate ai prospetti economico-patrimoniali, nonché ogni altra comunicazione relativa alla situazione economica, patrimoniale e finanziaria della società, i suddetti documenti devono essere redatti in base alle specifiche procedure aziendali in essere che:

- determinano con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili;
- prevedono la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema (anche informatico) che consente la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- prevedono criteri e modalità per l'elaborazione dei dati di bilancio e la trasmissione degli stessi da parte delle Società controllate alla controllante.

Con riferimento alle operazioni sul capitale sociale della Società, si segnala che le stesse, nonché l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle regole di *Corporate Governance* e delle procedure di Gruppo all'uopo predisposte.

* * *

Con particolare riferimento al reato di ***corruzione tra privat e istigazione alla corruzione tra privatii***, relativamente alle Attività Sensibili identificate al precedente paragrafo 13.2 devono essere rispettati inoltre i principi procedurali specifici qui di seguito descritti.

C) Gestione dei rapporti di alto profilo con soggetti privati

A presidio dell'Attività Sensibile in esame, la Società:

- verifica l'attendibilità ed onorabilità degli agenti/broker che collocano prodotti assicurativi per conto della Società (sulla base dell'accordo di collaborazione) prima dell'instaurazione del rapporto e, periodicamente, anche in costanza di rapporto;
- rende impossibile la modifica da parte dei tali soggetti delle condizioni contrattuali relative ai prodotti collocati in senso peggiorativo per il cliente finale (possibilità di concordare eventuali possibilità migliorative o peggiorative);
- monitora costantemente l'operato dei soggetti (in particolare Broker) che operano sulla base degli accordi di collaborazione con la Società.

D) Acquisto di beni, servizi e consulenze

1. i contratti tra APP Broker e le Società di Service e i Consulenti devono essere definiti per iscritto in tutte le loro condizioni e termini, e rispettare quanto indicato ai successivi punti;
2. nei contratti con i Consulenti deve essere contenuta apposita dichiarazione dei medesimi con cui si affermi: di essere a conoscenza della normativa di cui al D.Lgs. 231/2001 e delle sue implicazioni per la Società; di non essere mai stati implicati in procedimenti giudiziari relativi ai reati nello stesso contemplati (o se lo sono stati, devono comunque dichiararlo ai fini di una maggiore attenzione da parte della Società in caso si addivenga all'instaurazione del rapporto di consulenza);
3. nei contratti con i Consulenti deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto (es. clausole risolutive espresse, penali).

Inoltre a presidio dell'Attività Sensibile in esame, la Società:

- prevede livelli autorizzativi diversi a seconda dell'importo dell'acquisto;

- verifica l'attendibilità e l'onorabilità dei fornitori aziendali;
- attua una gara tra più fornitori per forniture superiori ad una soglia predeterminata ed indicata in apposita policy aziendale;
- prevede la tracciabilità dell'intero processo di gestione degli acquisti.

E) Gestione dei contenziosi

A presidio dell'Attività Sensibile in esame, la Società:

- definisce i ruoli e le responsabilità dei soggetti incaricati di gestire il singolo contenzioso o posizione pre - contenziosa;
- prevede la partecipazione di più soggetti al processo decisionale e la tracciabilità delle singole fasi di apertura e gestione del contenzioso e dei relativi accordi transattivi;
- prevede che il processo che conduce ad un accordo transattivo sia adeguatamente tracciato e che gli eventuali accordi transattivi siano debitamente formalizzati, sottoscritti in coerenza con il sistema autorizzativo in essere e correttamente archiviati;
- prevede che l'eventuale coinvolgimento di consulenti legali avvenga solo previa verifica dell'attendibilità e dell'onorabilità dei medesimi;
- prevede che la selezione dei legali esterni sia veicolata dall'Area Affari Legali di Allianz S.p.a.

Per la gestione dei contenziosi e delle conciliazioni, APP Broker si avvale del supporto dell'U.O. Affari legali di Allianz S.p.a.

F) Selezione e assunzione del personale dipendente

La Società adotta una procedura che disciplini l'interazione tra i diversi uffici coinvolti nella selezione e assunzione del personale.

La selezione e assunzione del personale è ispirata a un criterio di trasparenza sulla base dei seguenti parametri:

- professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
- uguaglianza di trattamento tra i diversi candidati;
- affidabilità rispetto al rischio di infiltrazione criminale.

La Società assicura che vengano prodotti prima dell'assunzione i seguenti documenti:

- *curriculum vitae;*
- casellario giudiziario;
- certificato dei carichi pendenti, non anteriore a tre mesi.

La Società conserva la documentazione esibita in sede di assunzione anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

G) Gestione dei flussi monetari e finanziari

La Società attua specifici controlli procedurali e cura con particolare attenzione i flussi che non rientrano nei processi tipici dell'azienda e che sono quindi gestiti in modo estemporaneo e discrezionale. La finalità di detti controlli consiste nell'impedire la formazione di riserve occulte o dazioni non giustificate di denaro o altre utilità che potrebbero essere il veicolo per la commissione di reati di corruzione.

Nessun pagamento può essere effettuato in contanti.

Sia gli agenti che i clienti sono obbligati all’utlilizzo del c/c di APP BROKER (conto Allianz Bank).

Si precisa che la tesoreria è gestita in outsourcing da Allianz S.p.A. per conto di APP Broker.

CAPITOLO 14 – DELITTI CON FINALITÀ DI TERRORISMO E DI EVERSIONE DELL'ORDINE DEMOCRATICO (Art. 25 quater del Decreto)

14.1. Le fattispecie dei delitti con finalità di terrorismo e di eversione dell'ordine democratico

Il presente capitolo si riferisce al Reato di Finanziamento del Terrorismo di cui D.lgs. 109/2007 e ai Reati con finalità di terrorismo e di eversione dell'ordine democratico di cui all'art. 25 *quater*.

In particolare, l'art.25 quater richiama i delitti aventi finalità di terrorismo o di eversione previsti dal codice penale e dalle leggi speciali, senza indicarli in modo specifico.

Tenuto conto dell'attività svolta dalla Società, si ritiene che, in relazione alla maggior parte di tali reati, non sia neppure astrattamente configurabile la commissione nell'interesse o a vantaggio della Società. Diversamente, meritano autonoma attenzione i reati di finanziamento del terrorismo, che saranno di seguito esaminati.

Si provvede, dunque, a fornire qui di seguito una breve descrizione del reato di Finanziamento del Terrorismo, in quanto ritenuto prima facie rilevante in relazione all'attività svolta dalla Società (cfr. Matrice delle attività a rischio-reato).

- ***FINANZIAMENTO DEL TERRORISMO***

Il Reato di Finanziamento del Terrorismo è stato introdotto con il D.lgs. 109/2007, di recepimento della direttiva 2005/60/CE emanata dal Parlamento europeo e dal Consiglio in data 26 ottobre 2005.

Per Finanziamento del Terrorismo, in base al D.Lgs. 109/2007 (recante "Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60 CE"), si intende: "*qualsiasi attività diretta, con qualsiasi mezzo, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, in qualunque modo realizzati, destinati ad essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo previsti dal codice penale, e ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti*".

La nuova normativa in tema di Finanziamento del Terrorismo adotta le medesime misure di prevenzione già vigenti contro i Reati di Riciclaggio ed introdotte con il Decreto Antiriciclaggio, prevedendo inoltre altre norme idonee per attuare il congelamento dei fondi e delle risorse economiche disposto dalle numerose risoluzioni del Consiglio di sicurezza delle Nazioni Unite che si sono succedute dal 1999 ad oggi, dal Regolamento CE n. 2580/2001 emanato dal Consiglio in data 27 dicembre 2001 e relativo a misure restrittive specifiche destinate a combattere il terrorismo, nonché dai Regolamenti comunitari emanati ai sensi degli artt. 60 e 301 del Trattato istitutivo della Comunità europea per il contrasto dell'attività dei Paesi che minacciano la pace e la sicurezza internazionale.

Il congelamento dei fondi e delle risorse economiche è disposto, con decreto, su proposta del Comitato di sicurezza finanziaria, dal Ministro dell'economia e delle finanze, di concerto con il Ministro degli affari esteri.

Ai sensi del D.lgs. 109/2007, per "*congelamento di fondi*" si intende il divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione del portafoglio. Per "*congelamento di risorse economiche*" si intende, invece, il divieto di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia.

14.2 Attività Sensibili

Le principali Attività Sensibili, che APP Broker ha individuato al proprio interno come rilevanti per la presente famiglia di reati, sono le seguenti.

A) Gestione dei flussi monetari e finanziari

L'Attività Sensibile in questione riguarda la gestione dei flussi monetari e finanziari della Società, con specifico riferimento alla gestione delle entrate (incassi, disinvestimenti di liquidità, etc.) e delle uscite (investimenti della liquidità, acquisti, consulenze, etc.).

B) Selezione e assunzione del personale dipendente

L'Attività Sensibile in questione è stata inserita in via prudenziale e riguarda il processo di assunzione e di selezione dei dipendenti della Società, anche con riferimento ad eventuale nuovo personale assunto in agenzia nel corso della gestione interinale della stessa.

C) Selezione delle controparti contrattuali

L'Attività Sensibile in questione riguarda il processo di Selezione delle controparti contrattuali, con particolare riferimento ai Consulenti e ai Fornitori.

14.3 Principi generali di comportamento

I Destinatari devono attenersi – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento di attività nelle Aree a Rischio individuate in precedenza – a regole di condotta conformi a quanto prescritto nel presente Modello e nelle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati di Riciclaggio, finanziamento del Terrorismo e con finalità di terrorismo o eversione dell'ordine democratico.
In particolare, i soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai Reati di Riciclaggio, finanziamento del terrorismo o con finalità di terrorismo o eversione dell'ordine democratico;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure aziendali interne in tutte le attività finalizzate alla gestione anagrafica di Fornitori;

4. assicurare un'approfondita conoscenza dei soggetti terzi con i quali vengono instaurati rapporti nell'esercizio del business aziendale, ovvero beneficiari di atti di disposizione del patrimonio libero della Società;
5. monitorare costantemente i flussi di denaro in uscita;
6. non effettuare alcuna operazione che possa presentare carattere anomalo per tipologia o oggetto ovvero che possa determinare l'instaurazione o il mantenimento di rapporti che presentino profili di anomalia dal punto di vista dell'affidabilità e/o della reputazione delle controparti;
7. non effettuare alcuna operazione – in via diretta o per il tramite di interposta persona – con soggetti, persone fisiche o giuridiche, residenti nella Lista Paesi predisposta dal Gruppo;
8. non riconoscere compensi a favore di Consulenti e Fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi o che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alla prassi vigenti in ambito locale;
9. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
10. non selezionare personale in azienda i cui requisiti e la cui affidabilità non sia stata adeguatamente esaminata, compatibilmente con la legislazione vigente.

Al fine dell'efficace attuazione di quanto sopra riportato, la Società adotta procedure in applicazione delle quali:

- i dati raccolti relativamente ai rapporti con clienti e Consulenti risultino completi ed aggiornati, sia per la corretta e tempestiva individuazione dei medesimi sia per una valida valutazione del loro profilo;
- la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia.

14.4 Principi specifici per le procedure

Ai fini dell'attuazione delle regole elencate al precedente paragrafo 14.3, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali specifici qui di seguito descritti.

A) Gestione dei flussi monetari e finanziari

Al fine di scongiurare il pericolo di commissione dei reati previsti nella presente Parte Speciale, è necessario:

- che qualunque transazione finanziaria presupponga la conoscenza del beneficiario della relativa somma;
- avere sempre conoscenza dell'utilizzo che verrà fatto dei fondi della Società gestiti da terzi.

Inoltre, non è ammesso l'utilizzo di risorse o di canali di pagamento non strettamente legati alla Società (per es. conti privati) per offrire indebite somme di denaro o fare offerte di altro genere o pagamenti vietati dai codici di Gruppo e dalle relative politiche e procedure aziendali.

Al fine dell'efficace attuazione di quanto sopra riportato, i Dipendenti, gli Organi Societari (nonché i Consulenti nella misura necessaria alle funzioni dagli stessi svolte) operano in base a procedure che consentano quanto segue:

• i dati raccolti relativamente ai rapporti con Consulenti devono essere completi ed aggiornati, sia per la corretta e tempestiva individuazione dei medesimi sia per una valida valutazione del loro profilo;

• la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia;

• siano posti in essere controlli sulle attività di selezione delle Controparti Contrattuali, dei Dipendenti, dei Consulenti e dei Fornitori;

• utlilizzo del c/c di APP BROKER (conto Allianz Bank).

Si precisa che la tesoreria è gestita in outsourcing da Allianz S.p.A. per conto di APP Broker

B) Selezione e assunzione del personale dipendente

Al fine di scongiurare il pericolo di commissione dei reati previsti nella presente Parte Speciale, è necessario:

- selezionare personale in azienda i cui requisiti e la cui affidabilità sia stata adeguatamente esaminata, compatibilmente con la legislazione vigente;
- che tra i programmi di formazione dei Dipendenti aventi ad oggetto il D.lgs.231/2001, uno specifico riferimento sia fatto alla trattazione dei Reati di finanziamento del terrorismo.

Al fine dell'efficace attuazione di quanto sopra riportato, i Dipendenti, gli Organi Societari (nonché i Consulenti nella misura necessaria alle funzioni dagli stessi svolte) operano in base a procedure che consentano quanto segue:

• i dati raccolti relativamente ai rapporti con Consulenti devono essere completi ed aggiornati, sia per la corretta e tempestiva individuazione dei medesimi sia per una valida valutazione del loro profilo;

• la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia;

• siano posti in essere controlli sulle attività di selezione delle Controparti Contrattuali, dei Dipendenti, dei Consulenti e dei Fornitori.

C) Selezione delle controparti contrattuali

1) La Società adotta una procedura aziendale per la gestione dei rapporti con i Fornitori, la quale preveda una verifica preliminare del possesso da parte degli stessi dei necessari requisiti di affidabilità e onorabilità.

2) La procedura di cui al precedente punto 1) disciplina altresì il processo di acquisto del bene, indicando le unità coinvolte, le modalità di richiesta di autorizzazione alla spesa e di effettuazione dei relativi pagamenti, nonché di contabilizzazione dell'importo.

3) La Società verifica periodicamente il possesso dei requisiti dell'affidabilità e onorabilità dei Fornitori.

4) La Società inserisce nei contratti con i Professionisti una specifica clausola con la quale gli stessi dichiarano i) di essere a conoscenza del D.Lgs 231/01 e di non essere mai incorsi nella commissione di uno dei reati in discorso, ii) di prendere atto che la Società ha adottato il presente Modello, pubblicato sul sito web, iii) si impegna al rispetto della normativa alla base del Modello e quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;

5) La Società inserisce nei contratti con Fornitori, Appaltatori e Broker una specifica clausola con la quale gli stessi dichiarano i) di essere a conoscenza del D.Lgs 231/01 e dichiara di non aver mai ricevuto condanne, anche non esecutive, per uno dei reati e degli illeciti amministrativi contemplati nel ciato Decreto, ii) di prendere atto che la Società ha adottato il presente Modello, pubblicato sul sito web, iii) si impegna al rispetto della normativa alla base del Modello e quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;

6) La Società inserisce nei contratti infragruppo una specifica clausola con la quale si dichiara e si garantisce che, nell'espletamento delle attività previste dal contratto, non sarà posto in essere - obbligandosi anche per il fatto del proprio personale ai sensi dell'art. 1381 del Codice Civile - alcun atto od omissione da cui possa derivare una responsabilità ai sensi del citato D.lgs. n. 231/2001, impegnandosi ad agire nel pieno rispetto del proprio Modello di Organizzazione, Gestione e Controllo ex Decreto 231;

7) Nei contratti con i Professionisti, i Fornitori, gli Appaltatori e i Broker, deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse);

8) Nei contratti con i Fornitori la Società inserisce altresì la specifica clausola *anti-corruption*.

9) La Società non intrattiene rapporti con Fornitori inseriti nelle *black list* pubblicate nel sito di Banca d'Italia e di altri organismi internazionali di prevenzione del terrorismo.

10) La Società non intrattiene rapporti con Fornitori residenti in un Paese inserito nelle liste dei Paesi Non Cooperativi (NCCT) pubblicate nel sito del FATF – GAFI (www.fatf-gafi.org).

11) La relazione sulla selezione dei consulenti e dei fornitori e l'evidenza delle eventuali criticità riscontrate in tale sede è oggetto di reportistica periodica nei confronti dell'OdV. Tale relazione contiene anche l'elenco dei soggetti cancellati dall'elenco dei fornitori per perdita dei requisiti di onorabilità e affidabilità o per presenza nelle liste internazionali sul terrorismo.

Al fine dell'efficace attuazione di quanto sopra riportato, i Dipendenti, gli Organi Societari (nonché i Consulenti nella misura necessaria alle funzioni dagli stessi svolte) operano in base a procedure che consentano quanto segue:

- i dati raccolti relativamente ai rapporti con Consulenti devono essere completi ed aggiornati, sia per la corretta e tempestiva individuazione dei medesimi sia per una valida valutazione del loro profilo;
- la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia;
- siano posti in essere controlli sulle attività di selezione delle Controparti Contrattuali, dei Dipendenti, dei Consulenti e dei Fornitori.

CAPITOLO 15 – REATI DI OMICIDIO COLPOSO E LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (Art. 25 septies del Decreto)

Il presente capitolo, intende disciplinare i comportamenti posti in essere dai componenti degli organi sociali e del management, dai dipendenti, nonché dai terzi che collaborano con la Società nello svolgimento dei processi a rischio (ad es.: fornitori, consulenti), al fine di prevenire la commissione dei reati contrari alla salute e alla sicurezza sul lavoro.

15.1. Le fattispecie dei reati di omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Il presente capitolo 15 si riferisce ai reati previsti dall'art. 25 *septies* del Decreto.

Tale articolo, originariamente introdotto dalla legge 3 agosto 2007 n. 123, e successivamente sostituito ai sensi dell'art. 300 del Decreto Sicurezza, fa riferimento ai reati di cui agli artt. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

L'inclusione nel novero dei reati-presupposto di fattispecie colpose - in materia di salute e sicurezza sul lavoro (art. 25 septies del decreto 231) e di ambiente (art. 25 undecies) - ha posto il problema della compatibilità logica tra la non volontà dell'evento, tipica degli illeciti colposi, e il finalismo sotteso al concetto di "interesse" dell'ente; ancora, è apparso assai difficle pensare, ad esempio, ad un vantaggio per l'ente connesso alla morte di un lavoratore.

Sul punto, le Sezioni Unite della Cassazione nella sentenza n. 38343 del 24.4.2014, emessa nell'ambito del processo cd. "Thyssen", hanno chiarito che "nei reati colposi di evento i concetti di interesse e vantaggio devono necessariamente essere riferiti alla condotta e non all'esito antigiuridico". Viene chiarito che tale soluzione "non determina alcuna difficoltà di carattere logico: è ben possibile che una condotta caratterizzata dalla violazione della disciplina cautelare e quindi colposa sia posta in essere nell'interesse dell'ente o determini comunque il conseguimento di un vantaggio. […] Tale soluzione interpretativa […] si limita ad adattare l'originario criterio d'imputazione al mutato quadro di riferimento, senza che i criteri d'ascrizione ne siano alterati. L'adeguamento riguarda solo l'oggetto della valutazione che, coglie non più l'evento bensì solo la condotta, in

conformità alla diversa conformazione dell'illecito. […] E' ben possibile che l'agente violi consapevolmente la cautela, o addirittura preveda l'evento che ne può derivare, pur senza volerlo, per corrispondere ad istanze funzionali a strategie dell'ente".

In relazione ai reati colposi, si potrà dunque ravvisare un interesse o un vantaggio dell'ente quando la violazione della regola di comportamento che ha prodotto l'evento sia stata dettata da esigenze aziendali, prima tra tutte il risparmio di spesa. Così, nel caso Thyssen, si è ravvisato un interesse dell'ente nel risparmio connesso alla mancata installazione di un adeguato sistema antincendio.

- **OMICIDIO COLPOSO (ART. 589 COD. PEN.)**

Il reato si configura ogni qualvolta un soggetto cagioni per colpa la morte di altro soggetto. Come già anticipato, il reato può essere fonte di responsabilità amministrativa dell'ente se sia stato commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

- **LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME (ART. 590 COMMA 3 COD. PEN.)**

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni ad altro soggetto lesioni gravi o gravissime. Ai sensi del comma 1 dell'art. 583 cod. pen. la lesione è considerata grave nei seguenti casi:

"*1) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;*

2) se il fatto produce l'indebolimento permanente di un senso o di un organo".

Ai sensi del comma 2 dell'art. 583 cod. pen., la lesione è considerata invece gravissima se dal fatto deriva:

- *"una malattia certamente o probabilmente insanabile;*

- *la perdita di un senso;*
- *la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;*
- *la deformazione, ovvero lo sfregio permanente del viso".*

Al fine di garantire l'adozione di un valido presidio avverso la potenziale commissione dei reati di cui all'art. 25 *septies* del Decreto, APP Broker ha deciso di adottare i principi previsti al presente capitolo 15, in conformità a quanto disposto dall'art. 30 del Decreto Sicurezza (d.lgs. n. 81/2008).
Nella predisposizione della presente Parte Speciale la Società ha tenuto conto dei principi cardine di cui alle Linee Guida Uni-Inail, al fine di garantire il rispetto da parte dei Destinatari di regole minime di comportamento in relazione alla determinazione della politica aziendale in tema di sicurezza, alla relativa pianificazione degli obiettivi, alla messa in atto di opportune azioni di monitoraggio, alla sensibilizzazione del personale ed, infine, al periodico riesame del sistema in essere al fine di valutarne la sua efficacia ed efficienza.

15.2 Attività Sensibili

La principale Attività Sensibile, che APP Broker ha individuato al proprio interno come rilevante per la presente famiglia di reati, è la seguente:

A) Espletamento e gestione degli adempimenti in materia di tutela della salute e sicurezza sul lavoro

L'Attività Sensibile in questione riguarda l'espletamento e gestione degli adempimenti in materia di tutela della salute e sicurezza sul lavoro ai sensi del D.lgs. 81/2008 (Testo Unico Sicurezza) e successive modifiche ed integrazioni, con particolare riferimento:

- alle attività di ufficio e/o d'impresa svolta dal personale dipendente (in particolare per ciò che concerne la conformità delle attrezzature ai requisiti normativi);
- prevenzione incendi e piani di evacuazione..

15.3 Principi generali di comportamento

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- Documento di Valutazione dei Rischi con i relativi documenti integrativi;
- le procedure operative ed organizzative in materia di salute e sicurezza sul lavoro, ad esempio relative a:
    - valutazione dei rischi per la salute e sicurezza sul lavoro;
    - sistema di segnalazione dei rischi;
    - Sorveglianza Sanitaria;
    - modalità di consultazione del RLS;
    - Piano di Emergenza.

È previsto a carico dei Destinatari, l'espresso divieto di porre in essere, promuovere, collaborare, o dare causa a comportamenti tali da integrare fattispecie di reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies* del Decreto).

15.4 Principi specifici per le procedure

Al fine di consentire l'attuazione dei principi finalizzati alla tutela della salute e della sicurezza dei Lavoratori, così come individuati dal Decreto Sicurezza, si prevede quanto segue.

15.4.1 La politica aziendale in tema di sicurezza

La politica per la sicurezza e salute sul lavoro adottata da APP Broker si pone come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte sul luogo di lavoro, nell'ottica della salute e sicurezza di tutti i Lavoratori e al fine di prevenire o quanto meno limitare il rischio di verificazione di un reato commesso in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Tale politica deve contenere:

- una chiara affermazione della responsabilità dell'intera organizzazione aziendale, dal Datore di Lavoro al singolo Lavoratore, nella gestione delle tematiche relative alla salute e sicurezza sul lavoro, ciascuno per le proprie attribuzioni e competenze;
- l'impegno a considerare tali tematiche come parte integrante della gestione aziendale, e ad assegnare alla tutela della salute e della sicurezza carattere prioritario rispetto alla finalità di profitto;
- l'impegno al miglioramento continuo ed alla prevenzione;
- l'impegno a fornire le risorse umane, economiche e strumentali necessarie;
- l'impegno a garantire che i Destinatari, nei limiti delle rispettive attribuzioni, siano sensibilizzati a svolgere la propria attività nel rispetto delle norme sulla tutela della salute e sicurezza;
- l'impegno al coinvolgimento ed alla consultazione dei Lavoratori, anche attraverso il RLS;
- l'impegno ad un riesame periodico della politica per la salute e sicurezza adottato al fine di garantire la sua costante adeguatezza alla struttura organizzativa aziendale.

15.4.2 Il processo di pianificazione

APP Broker, anche per il tramite di Società di Service, con cadenza periodica, nell'ambito di una pianificazione di Gruppo:

- definisce un programma di sopralluoghi in tutti i contesti aziendali in cui sussistono rischi in materia di salute e sicurezza nei luoghi di lavoro;
- definisce un piano di interventi per l'eliminazione o la riduzione dei rischi sopra richiamati anche con riferimento al rischio stress lavoro correlato;
- definisce gli obiettivi finalizzati al mantenimento e/o miglioramento delle misure di prevenzione e protezione stabilendo un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità;
- definisce le risorse (e le relative modalità di gestione), anche economiche, necessarie;

- prevede le modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi.

15.4.3 L'organizzazione del sistema

A) Compiti e responsabilità

Nella definizione dei compiti organizzativi ed operativi dei Lavoratori, devono essere esplicitati e resi noti anche quelli relativi alle attività di sicurezza di loro competenza, nonché le responsabilità connesse all'esercizio delle stesse ed i compiti di ispezione, verifica e sorveglianza in materia di SSL.

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti.

Al fine di garantire un'attuazione ancor più efficiente e puntuale della politica aziendale in materia di sicurezza, APP Broker elabora un sistema informativo in cui è prevista - e costantemente aggiornata - una precisa definizione dei compiti e delle responsabilità spettanti alle singole funzioni aziendali in materia di SSL.

Il Datore di Lavoro

Al Datore di Lavoro sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti compiti non delegabili:

1) valutare tutti i rischi per la sicurezza e per la salute dei lavoratori (incluso il rischio stress lavoro correlato);

2) elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi con data certa (da custodirsi presso l'azienda) contenente tra l'altro:

- una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa;
- l'indicazione delle eventuali misure di prevenzione e di protezione attuate e degli eventuali dispositivi di protezione individuale adottati a seguito della suddetta valutazione dei rischi (artt. 74-79 del Decreto Sicurezza);

- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere;
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici e che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

L'attività di valutazione e di redazione del documento, pianificata nell'ambito della riunione periodica annuale prevista dall'art. 35 del Decreto Sicurezza ed effettuata anche mediante appositi sopralluoghi negli ambienti di lavoro e con l'ausilio di strumenti di valutazione specifica per lo stress lavoro correlato, deve essere compiuta in collaborazione con il RSPP e con il Medico Competente.

La valutazione dei rischi è oggetto di consultazione preventiva con il Rappresentante dei Lavoratori per la Sicurezza;

3) designare il Responsabile del Servizio di Prevenzione.

Al Datore di Lavoro sono attribuiti numerosi altri compiti dallo stesso delegabili a soggetti qualificati. Tali compiti, previsti dal Decreto Sicurezza, riguardano, tra l'altro: a) la nomina del Medico Competente per l'effettuazione della Sorveglianza Sanitaria; b) la designazione preventiva dei Lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione delle emergenze; c) l'adempimento degli obblighi di informazione, formazione ed addestramento; d) la convocazione della riunione periodica annuale di cui all'art. 35 del Decreto Sicurezza (la quale ha altresì luogo anche in occasione di eventuali significative variazioni delle condizioni di esposizione al rischio, compresa la programmazione e l'introduzione di nuove tecnologie che hanno riflessi sulla sicurezza e salute dei lavoratori).; e) l'aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi che hanno rilevanza ai fini della salute e sicurezza del lavoro, etc.

In relazione a tali compiti, ed a ogni altro compito affidato al Datore di Lavoro che possa essere da questi delegato[2] ai sensi del Decreto Sicurezza, la suddetta delega[3] è ammessa con i seguenti limiti e condizioni che:

- esso risulti da atto scritto recante data certa;
- il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
- essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate.

Al fine di garantire l'attuazione di un modello di sicurezza aziendale sinergico e compartecipativo, il Datore di Lavoro fornisce al Servizio di Prevenzione e Protezione ed al Medico Competente informazioni in merito a:

a) la natura dei rischi;

b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;

c) la descrizione dei luoghi di lavoro e degli eventuali processi produttivi;

d) i dati relativi agli infortuni e quelli relativi alle malattie professionali;

e) tutti i dati relativi al personale, utili per la valutazione dello stress lavoro correlato.

Il Datore di Lavoro – o, in caso di delega di funzioni, il suo delegato e i dirigenti, – devono vigilare sull'adempimento degli obblighi che, in base alle disposizioni del Decreto Sicurezza, spettano a i) preposti ii) lavoratori iii) progettisti iv) fabbricanti v) fornitori vi) installatori vii) medico competente.

[2] In base all'art. 299 del Decreto Sicurezza, si ricorda che "*Le posizioni di garanzia relative ai soggetti di cui all'art.2, comma 1, lettere b,d,e (Datore di Lavoro, Dirigente e Preposto) gravano altresì su colui il quale, pur sprovvisto di regolare investitura, eserciti in concreto i poteri giuridici riferiti a ciascuno dei soggetti ivi definiti*".

[3] La delega di funzioni non esclude l'obbligo di vigilanza in capo al Datore di Lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. L'obbligo di cui al primo periodo si intende assolto in caso di adozione ed efficace attuazione del modello di verifica e controllo di cui all'articolo 30, comma 4. del Decreto Sicurezza.

Il Servizio di Prevenzione e Protezione (SPP)

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro si avvale, ricorrendo anche a soggetti esterni, del Servizio di Prevenzione e Protezione dei rischi professionali che provvede:

- all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- a elaborare, per quanto di competenza, le misure preventive e protettive a seguito della valutazione dei rischi e i sistemi di controllo di tali misure;
- a elaborare le procedure di sicurezza per le varie attività aziendali;
- a proporre i programmi di informazione e formazione dei Lavoratori;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'art. 35 del Decreto Sicurezza;
- a fornire ai Lavoratori ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria, in relazione ai diversi ambiti di rischio.

Qualora nell'espletamento dei relativi compiti, il RSPP verificasse la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro, il RSPP dovrà darne immediata comunicazione all'OdV.

L'eventuale sostituzione del RSPP dovrà altresì essere comunicata all'OdV con l'espressa indicazione delle motivazioni a supporto di tale decisione.

Il RSPP deve avere capacità e requisiti professionali in materia di prevenzione e sicurezza e, precisamente deve:

- essere in possesso di un titolo di istruzione secondaria superiore;
- aver partecipato a specifici corsi di formazione adeguati alla natura dei rischi presenti sul luogo di lavoro ivi compreso lo stress lavoro correlato;
- aver conseguito attestato di frequenza di specifici corsi di formazione in materia di prevenzione e protezione dei rischi;

- aver frequentato corsi di aggiornamento.

Il RSPP è coinvolto regolarmente ed è invitato alle riunioni dell'OdV.

Il Medico Competente

Il Medico Competente provvede tra l'altro a:

- collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della Sorveglianza Sanitaria (come descritta nel successivo paragrafo b), alla predisposizione della attuazione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori, all'attività di formazione ed informazione nei loro confronti, per la parte di competenza, e all'organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- programmare ed effettuare la Sorveglianza Sanitaria;
- istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ogni Lavoratore sottoposto a Sorveglianza Sanitaria;
- fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informandoli sui relativi risultati;
- comunicare per iscritto in occasione della riunione periodica di cui all'art. 35 del Decreto Sicurezza i risultati anonimi collettivi della Sorveglianza Sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica dei lavoratori;
- visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa in base alla valutazione di rischi.

Il Medico Competente deve essere in possesso di uno dei titoli ex art. 38 D.Lgs. 81/2008 e, precisamente:

- di specializzazione in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica, o in tossicologia industriale, o in igiene industriale, o in fisiologia ed igiene del

lavoro, o in clinica del lavoro ed altre specializzazioni individuate, ove necessario, con decreto del Ministro della Sanità di concerto con il Ministro dell'Università e della Ricerca Scientifica e Tecnologica.

oppure

- essere docente o libero docente in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica, o in tossicologia industriale, o in igiene industriale, o in fisiologia ed igiene del lavoro;
- essere in possesso dell'autorizzazione di cui all'articolo 55 del D.Lgs. 277/91 che prevede una comprovata esperienza professionale di almeno 4 anni.

Il Rappresentante dei Lavoratori per la Sicurezza (RLS)

È il soggetto eletto o designato, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro.

Riceve, a cura del Datore di Lavoro o di un suo delegato, la prevista formazione specifica in materia di salute e sicurezza.

Il RLS:

- accede ai luoghi di lavoro;
- è consultato preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- è consultato sulla designazione del RSPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso e del Medico Competente;
- è consultato in merito all'organizzazione delle attività formative;
- promuove l'elaborazione, l'individuazione e l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei lavoratori;
- partecipa alla "riunione periodica di prevenzione e protezione dai rischi";

- riceve informazioni inerenti la valutazione dei rischi e le misure di prevenzione relative e, ove ne faccia richiesta e per l'espletamento della sua funzione, copia del Documento di Valutazione dei Rischi.

Il RLS dispone del tempo necessario allo svolgimento dell'incarico, senza perdita di retribuzione, nonché dei mezzi necessari per l'esercizio delle funzioni e delle facoltà riconosciutegli; non può subire pregiudizio alcuno a causa dello svolgimento della propria attività e nei suoi confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.

I Lavoratori

È cura di ciascun Lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite.

I Lavoratori devono in particolare:

- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro o dal suo delegato ai fini della protezione collettiva ed individuale;
- utilizzare correttamente le apparecchiature da lavoro nonché gli eventuali dispositivi di sicurezza;
- segnalare immediatamente al Datore di Lavoro le deficienze dei mezzi e dei dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al Rappresentante dei Lavoratori per la Sicurezza;
- partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;
- sottoporsi ai controlli sanitari previsti nei loro confronti;
- contribuire, insieme al Datore di Lavoro o al suo delegato all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

I lavoratori di aziende che svolgono per APP Broker attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

Nel caso di lavori in appalto, ad esempio ai sensi dell'art.26 o del Titolo IV del d.lgs.n.81/2008, possono inoltre essere presenti ulteriori figure:

Il Committente

Il Committente, tra l'altro:

- si attiene, nella fase di progettazione dell'opera ed in particolare al momento delle scelte tecniche, nell'esecuzione del progetto e dell'organizzazione del Cantiere, ai principi e alle misure generali di tutela di cui all'articolo 15 del Decreto Sicurezza;
- prevede nel progetto, al fine di permettere la pianificazione dell'esecuzione in condizioni di sicurezza dei lavori o delle fasi di lavoro che si debbono svolgere simultaneamente o successivamente tra loro, la durata di tali lavori o fasi di lavoro;
- valuta, nella fase di progettazione dell'opera il Piano di Sicurezza e Coordinamento e il Fascicolo dell'Opera;
- prima dell'affidamento dei lavori designa, ove necessario, il Coordinatore per la Progettazione previa verifica del possesso dei requisiti di cui all'art. 98 del Decreto Sicurezza. La designazione dovrà essere formalizzata con comunicazione scritta;
- verifica l'adempimento degli obblighi da parte del Coordinatore per la Progettazione;
- prima dell'affidamento dei lavori designa, ove necessario, il Coordinatore per l'Esecuzione dei Lavori. La designazione dovrà essere formalizzata con comunicazione scritta;
- comunica alle imprese esecutrici e ai Lavoratori autonomi il nominativo del Coordinatore per la Progettazione e quello del Coordinatore per l'Esecuzione dei Lavori;
- verifica l'idoneità tecnico-professionale delle imprese esecutrici e dei Lavoratori autonomi in relazione ai lavori da affidare, anche attraverso l'iscrizione alla camera di commercio, industria e artigianato e del documento unico di regolarità contributiva corredato da autocertificazione in ordine al possesso dei requisiti di cui all'allegato XVII del Decreto Sicurezza.

Il Committente è esonerato dalle responsabilità connesse all'adempimento degli obblighi limitatamente all'incarico conferito al Responsabile dei Lavori (purché l'incarico risulti comunque attribuito a persona capace e competente). In ogni caso il conferimento dell'incarico non esonera il Committente dalle responsabilità connesse alle verifiche degli adempimenti degli obblighi di cui agli articoli 90, 92, comma 1, lettera e), e 99 del Decreto Sicurezza.

Il Responsabile dei Lavori

E' il soggetto che può essere incaricato dal Committente della progettazione o controllo dell'esecuzione dell'opera. Ad esso, se nominato, competono gli obblighi che il titolo IV del Decreto Sicurezza pone in capo al Committente.

Il Coordinatore per la Progettazione

Il Coordinatore per la Progettazione, che deve essere in possesso dei requisiti professionali previsti dal Decreto Sicurezza, tra l'altro:

- redige, durante la fase di progettazione dell'opera e comunque prima della richiesta di presentazione delle offerte, il PSC;
- predispone il Fascicolo dell'Opera, contenente le informazioni utili ai fini della prevenzione e della protezione dai rischi cui sono esposti i Lavoratori.

Il Coordinatore per l'Esecuzione

Il Coordinatore per l'Esecuzione, tra l'altro:

- verifica, con opportune azioni di coordinamento e controllo, l'applicazione, da parte delle imprese esecutrici e dei Lavoratori autonomi, delle disposizioni di loro pertinenza contenute nel PSC e la corretta applicazione delle relative procedure di lavoro;

- verifica l'idoneità del POS, da considerare come piano complementare di dettaglio del PSC assicurandone la coerenza con quest'ultimo, adegua il PSC ed il Fascicolo dell'Opera in relazione all'evoluzione dei lavori e alle eventuali modifiche intervenute, valutando le proposte delle imprese esecutrici dirette a migliorare la sicurezza in Cantiere e verifica che le imprese esecutrici adeguino, se necessario, i rispettivi POS;
- organizza tra i datori di lavoro, ivi compresi i Lavoratori autonomi, la cooperazione ed il coordinamento delle attività nonché la loro reciproca informazione;
- segnala al Committente e al Responsabile dei Lavori, se designato, previa contestazione scritta alle imprese ed ai Lavoratori autonomi interessati, le inosservanze agli obblighi a carico dei Lavoratori autonomi, dei datori di lavoro delle imprese esecutrici e dei rispettivi Dirigenti e Preposti di cui agli artt. 94, 95 e 96 del Decreto Sicurezza, nonché alle prescrizioni del PSC e propone la sospensione dei lavori, l'allontanamento delle imprese esecutrici o dei Lavoratori autonomi dal Cantiere o la risoluzione del relativo contratto, dandone comunicazione all'OdV. In caso di non intervento del Committente e del Responsabile dei Lavori comunica le inadempienze alla ASL e DPL di competenza;
- sospende, in caso di pericolo grave e imminente, direttamente riscontrato, le singole lavorazioni fino alla verifica degli avvenuti adeguamenti effettuati dalle imprese effettuate;
- segnala all'OdV la sussistenza di qualsiasi criticità riscontrata nell'adempimento delle proprie funzioni (es. inosservanza di obblighi da parte delle imprese esecutrici, sospensione dei lavori, etc.).

B) Sorveglianza Sanitaria

La gestione delle attività di sorveglianza sanitaria, prevede in via prioritaria, la nomina del Medico Competente aziendale, previo accertamento della presenza dei titoli e requisiti necessari allo svolgimento dell'incarico, secondo quanto stabilito all'art. 38 del Decreto Sicurezza.

Per consentire il rispetto degli obblighi di legge, APP Broker prevede nel DVR e nel protocollo sanitario procedure specifiche, concernenti l'espletamento dell'attività di sorveglianza sanitaria nei confronti di:

- Lavoratori che utilizzano attrezzature munite di Videoterminali così come definiti dall'art.173 punto c del Decreto Sicurezza;
- Lavoratrici in stato di gravidanza;

- Lavoratori portatori di *handicap*;
- Lavoratori soggetti alla movimentazioni manuale dei carichi così come definiti nel Titolo VI del Decreto Sicurezza;
- Lavoratori esposti ad agenti fisici, biologici e sostanze pericolose;
- Lavoratori esposti ad eventuali rischi da stress lavoro-correlato e *mobbing*.

Di particolare rilevanza risulta essere la gestione delle attività di sorveglianza sanitaria in relazione ai seguenti aspetti:

- trasmissione dell'elenco dei lavoratori esposti al Medico Competente;
- tipologia di lavoratori sottoposti a sorveglianza sanitaria;
- attività di pianificazione delle visite dei lavoratori "esposti" (andrebbero definiti);
- struttura della relazione del Medico Competente contenente i dati relativi alla popolazione aziendale (relazione anonima da presentare durante la riunione periodica e relazione da inviare all'OdV da parte del Medico Competente);
- modalità di registrazione ed archiviazione delle informazioni.

C) Informazione e formazione

C1) Informazione

L'informazione che APP Broker riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a:

a) le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle regole adottate da APP Broker in tema di SSL;

b) il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di sicurezza e ogni altra prescrizione relativa al sistema di SSL adottato da APP Broker, nonché ai principi indicati nella presente Parte Speciale.

Ciò premesso, APP Broker, anche per il tramite di Società di Service, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun Dipendente, è tenuta ai seguenti oneri informativi:

- deve essere fornita adeguata informazione ai dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) circa i rischi specifici dell'impresa, per quanto limitati, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;
- deve essere data evidenza dell'informativa erogata per la gestione del pronto soccorso, emergenza, evacuazione e prevenzione incendi e devono essere verbalizzati gli eventuali incontri;
- deve essere data adeguata informativa circa i contenuti delle procedure aziendali adottate per la gestione della sicurezza e salute dei Lavoratori;
- i dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) devono ricevere informazione sulla nomina del RSPP, sul Medico Competente e sugli addetti ai compiti specifici per il pronto soccorso, salvataggio, evacuazione e prevenzione incendi;
- deve essere formalmente documentata l'informazione e l'istruzione per l'uso delle attrezzature di lavoro messe a disposizione dei Lavoratori;
- devono essere evidenziati i pericoli connessi all'uso delle sostanze e dei preparati pericolosi;
- il RSPP e/o il Medico Competente devono essere coinvolti nella definizione delle informazioni;
- APP Broker deve organizzare periodici incontri tra le funzioni preposte alla sicurezza sul lavoro;
- APP Broker deve coinvolgere il Rappresentante dei Lavoratori per la Sicurezza nella organizzazione della attività di rilevazione e valutazione dei rischi, nella designazione degli addetti alla attività di prevenzione incendi, pronto soccorso ed evacuazione.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione.

C2) Formazione

APP Broker deve fornire adeguata formazione a tutti i dipendenti in materia di sicurezza sul lavoro, con specifico riferimento a:

- concetti di rischio, danno, prevenzione, protezione, uso dei DPI, organizzazione della prevenzione aziendale, diritti e doveri dei vari soggetti aziendali, organi di vigilanza, controllo, assistenza;

- rischi riferiti alle mansioni, ai possibili danni e alle conseguenti misure e procedure di prevenzione e di protezione caratteristici del settore o del comparto di appartenenza dell'azienda.

La suddetta attività di formazione deve essere assicurata:

- al momento della costituzione del rapporto di lavoro;
- in occasione di trasferimenti o cambiamento di mansioni;
- in caso di introduzione di nuove attrezzature o strumenti di lavoro, di nuove tecnologie o di sostanze pericolose.

Con riferimento all'attività di Formazione, valgano altresì le seguenti considerazioni:

- Il RSPP e/o il Medico Competente devono partecipare alla stesura del piano di formazione;
- la formazione erogata deve prevedere questionari di valutazione;
- la formazione deve essere adeguata ai rischi della mansione cui il Lavoratore è in concreto assegnato;
- gli addetti a specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al pronto soccorso, RLS) devono ricevere specifica formazione;
- i Dirigenti e i Preposti devono ricevere specifica formazione in relazione ai propri compiti in materia di SSL.

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione, e deve essere ripetuta periodicamente.

La partecipazione all'attività di formazione è obbligatoria; la mancata partecipazione non giustificata comporterà l'irrogazione di una sanzione disciplinare che sarà comminata secondo le regole indicate nel capitolo 8 della Parte Generale del presente Modello.

D) Comunicazione, flusso informativo e cooperazione

Al fine di garantire maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, APP Broker si organizza per garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Lavoratori.

A tal proposito APP Broker adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

a) dal basso verso l'alto

Il flusso dal basso verso l'alto è garantito da APP Broker mettendo a disposizione apposite schede di segnalazione attraverso la compilazione delle quali ciascuno dei Lavoratori ha la possibilità di portare a conoscenza del proprio superiore gerarchico o direttamente dell'RLS osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale;

b) dall'alto verso il basso

Il flusso dall'alto verso il basso ha lo scopo di diffondere a tutti i Lavoratori le politiche, gli obiettivi, i programmi e i risultati in materia di salute e sicurezza sui luoghi di lavoro.

A tale scopo APP Broker garantisce ai Destinatari un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente.

E) Documentazione

APP Broker, anche per il tramite di Società di Service, dovrà provvedere a conservare, sia su supporto cartaceo che informatico, i seguenti documenti:

- la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita secondo le modalità concordate con il Datore di Lavoro;
- il Documento di Valutazione dei Rischi che contiene il programma delle misure di mantenimento e di miglioramento ed è lo strumento fondamentale che permette al Datore di Lavoro di individuare le misure di prevenzione e protezione e di pianificarne l'attuazione.

APP Broker è altresì chiamata a garantire che:

- il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente;
- venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica;
- venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale;
- venga conservata ogni procedura adottata da APP Broker per la gestione della salute e sicurezza sui luoghi di lavoro;
- venga conservato e aggiornato il Registro delle Manutenzioni;
- tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell' OdV.

APP Broker provvede in ogni caso a conservare ogni altra documentazione e certificazione obbligatoria per legge.

F) Rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici

Al fine di ottemperare agli obblighi previsti dalla normativa vigente in materia di salute e sicurezza negli ambienti di lavoro, in particolar modo con riferimento al rispetto degli standard tecnico-strutturali di legge, APP Broker adotta delle procedure volte a garantire una corretta gestione nel tempo delle strutture aziendali (locali, arredi, macchinari, ecc.) e una periodica valutazione sanitaria degli ambienti di lavoro.

La Società, in aggiunta a quanto previsto nel precedente paragrafo E, con specifico riferimento al rispetto degli standard tecnico strutturali, predispone e aggiorna, tra l'altro, la documentazione di seguito elencata:

- Certificato di agibilità e abilità e planimetrie di dettaglio dei locali;
- Dichiarazione di conformità impianto elettrico ed impianto di protezione scariche atmosfere ed evidenza dell'invio delle stesse ad ASL;

- Licenza d'uso e nulla osta alla Dichiarazione Inizio Attività Produttiva;
- Incarico ad organismo notificato per le verifiche periodiche dell' impianto di messa a terra e dell'impianto di protezione scariche atmosferiche;
- manuali e le istruzioni per l'uso di macchine, attrezzature ed eventuali dispositivi di protezione individuale forniti dai costruttori;
- Dichiarazione di conformità impianto distribuzione e allacciamento gas;
- Contratto di allacciamento per approvvigionamento idrico;
- Autorizzazione allo scarico delle acque reflue civili e meteoriche con relativa planimetria della rete fognaria;
- Certificato Prevenzione Incendi relativi progetti vidimati dai Vigili del Fuoco;
- Certificato di reazione al fuoco dei materiali adottati per le superfici esposte a rischio incendio;
- Dichiarazione di conformità delle attrezzature antincendio adottate (estintori, idranti, rilevatori, compartimentazione, ecc);
- Documentazione tecnica di dichiarazione di conformità su flussi aria, temperatura, umidità;
- Dichiarazione di conformità apparecchi a pressione (serbatoi, autoclavi);
- Libretti di centrale per impianti termici;
- Dichiarazione di conformità dell'impianto idraulico ed invio della denuncia all'ISPESL per impianti termici ad acqua calda con potenza superiore a 35 KW;
- Certificazioni cablaggi linee di rete;
- Libretti di impianto, contratto di manutenzione con ditta abilitata e verbale di nomina dell'organismo notificato per ascensori/montacarichi;
- Libretti d'impianto per le apparecchiature di refrigerazione condizionamento contenenti sostanze lesive dell'ozono.

G) Gestione delle emergenze e primo soccorso

Le situazioni d'emergenza sono gestite secondo quanto indicato nel Piano d'Emergenza redatto, ed aggiornato a cura del Servizio Prevenzione e Protezione e del suo Responsabile.

A tal proposito si segnala che all'interno del Piano di Emergenza sono individuate le figure preposte alla gestione delle emergenze sia "antincendio" che di "primo soccorso", nonché gli incaricati della gestione delle relative esercitazioni.

Esercitazioni antincendio

Secondo quanto previsto dalla normativa vigente, presso ciascuna sede aziendale, le figure identificate nel Piano d'Emergenza organizzano un'esercitazione antincendio annuale al fine di mettere in pratica le procedure di evacuazione e di verificare la corretta applicazione delle istruzioni riportate nel Piano d'Emergenza.

La gestione del Primo Soccorso

Il Datore di Lavoro, coordinandosi con il Medico Competente, adotta i provvedimenti necessari al fine di garantire una efficiente gestione delle attività di primo soccorso.
In base all'art. 45 del Decreto Sicurezza, le caratteristiche minime delle attrezzature di primo soccorso, i requisiti del personale addetto e la sua formazione, individuati in relazione alla natura dell'attività al numero dei lavoratori occupati ed ai fattori di rischio, sono individuati dal Decreto Ministeriale 15 luglio 2003 n.388 e dai successivi decreti ministeriali di adeguamento.

H) L'attività di monitoraggio

APP Broker deve assicurare un costante ed efficace monitoraggio delle misure di prevenzione e protezione adottate sui luoghi di lavoro, della loro corretta applicazione, nonché del rispetto degli standard tecnico-strutturali di cui al precedente paragrafo F.

A tale scopo APP Broker, in coordinamento con l'Organismo di Vigilanza:

- assicura un costante monitoraggio delle misure preventive e protettive (e della loro attuazione) predisposte per la gestione della salute e sicurezza sui luoghi di lavoro, (art. 28, comma 2 lettera c, D.lgs. 81/08), nonché la definizione dei ruoli dell'organizzazione aziendale che debbano provvedere alla loro attuazione (art. 28, comma 2 lettera d, D.lgs. 81/08);
- assicura la presenza di tutta la documentazione necessaria per legge in materia di salute e sicurezza sui luoghi di lavoro;

- assicura un costante monitoraggio dell'adeguatezza e della funzionalità di tali misure a raggiungere gli obiettivi prefissati e della loro corretta applicazione;
- assicura un costante monitoraggio dell'attuazione delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere.

L'attività di monitoraggio viene assicurata attraverso il rispetto delle norme interne che prevedono:

- i ruoli ed i compiti dei soggetti responsabili delle seguenti attività:
  - emissione di procedure ed istruzioni in materia di salute e sicurezza sui luoghi di lavoro;
  - verifica del buon funzionamento nel tempo degli impianti aziendali in materia di salute e sicurezza sui luoghi di lavoro, della loro manutenzione e della loro revisione;
  - ricevimento di eventuali segnalazioni di mal funzionamento, vetustà o inefficienza degli impianti e dei macchinari stessi;
- l'acquisizione da parte dell'Organismo di Vigilanza, in qualunque momento e senza necessità di autorizzazione, di tutta la documentazione relativa ai controlli sulle procedure e le istruzioni di sicurezza;
- il monitoraggio sui manuali di *security*;
- il controllo sullo svolgimento dei piani aziendali di informazione e formazione;
- l'emanazione delle istruzioni relative all'utilizzo delle attrezzature munite di videoterminali;
- la tempistica e la comunicazione dei risultati riscontrati;
- il sistema sanzionatorio applicato in caso di violazione delle misure in materia di salute e sicurezza sui luoghi di lavoro.

Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta, APP Broker, laddove la specificità del campo di intervento lo richiedesse, fa affidamento a risorse esterne con elevato livello di specializzazione.

APP Broker garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.

l) Il riesame del sistema

Al termine dell'attività di monitoraggio di cui alla precedente paragrafo, il sistema adottato da APP Broker per la gestione della salute e sicurezza dei lavoratori è sottoposto ad un riesame periodico da parte del Datore di Lavoro, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati.

L'attività di riesame in commento, dovrà tra l'altro basarsi su:

- statistiche infortuni;
- statistiche riconducibili allo stress lavoro correlato;
- risultato dell'attività di monitoraggio effettuata;
- azioni correttive intraprese;
- rapporti sulle emergenze;
- segnalazioni pervenute dall'OdV.

Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.

CAPITOLO 16 – RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHE' DI AUTORICICLAGGIO (Art. 25 octies del Decreto)

16.1. Le fattispecie dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio

Il presente capitolo 16 si riferisce ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio di cui all'art. 25 *octies* del D.lgs. 231/2001 (introdotti dal Decreto Antiriciclaggio).

Si descrivono brevemente qui di seguito le singole fattispecie della presente famiglia di reati ritenute applicabili, anche se in via prudenziale, data l'operatività di APP Broker.

- **RICICLAGGIO (ART. 648 BIS C.P.)**

Tale ipotesi di reato si configura nel caso in cui un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Per "sostituzione" si intende la condotta consistente nel cambiare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi.

Per "trasferimento" si intende la condotta consistente nello spostamentodidenaro, beni o altre utilità, anche mediante il compimento di atti negoziali.

Per la realizzazione di tale reato, dunque, è richiesto un quid pluris rispetto al reato di ricettazione, ovvero il compimento di attività idonee a celare l'origine illecita dei proventi.

Non può essere autore del reato chi abbia commesso o concorso a commettere il delitto dal quale provengono le utilità riciclate.

- **IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 648 TER C. P.)**

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto.

La punibilità per tale reato è prevista solo per coloro i quali non siano già compartecipi del reato principale.

Il reato non si configura se il fatto costituisce già ricettazione o riciclaggio.

A differenza del riciclaggio, l'impiego non richiede che la condotta sia in grado di ostacolare l'identificazione della provenienza delittuosa del bene.

Il termine "impiegare" è normalmente sinonimo di "utilizzo per qualsiasi scopo". Tuttavia, considerato che il fine ultimo perseguito dal legislatore consiste nell'impedire il turbamento del sistema economico e dell'equilibrio concorrenziale attraverso l'utilizzo di capitali illeciti reperibili a costi inferiori rispetto a quelli leciti, si ritiene che per "impiegare" debba intendersi in realtà "investire". Pertanto, dovrebbe ritenersi rilevante un utilizzo a fini di profitto.

Premesso che presupposto comune di tutte e tre le fattispecie incriminatrici di cui agli artt. 648, 648 bis e 648 ter c.p. è quello costituito dalla provenienza da delitto del denaro o di qualsiasi altra utilità di cui l'agente sia venuto a disporre, si precisa che tali fattispecie si distinguono sotto il profilo soggettivo, per il fatto che la prima di esse richiede, oltre alla consapevolezza della su indicata provenienza, necessaria anche per le altre, solo una generica finalità di profitto, mentre la seconda o la terza richiedono la specifica finalità di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità, quanto alla terza, che detta finalità deve essere perseguita mediante l'impiego delle risorse in attività economiche o finanziarie.

- **AUTORICICLAGGIO (ART. 648 TER.1 C.P.)**

La nuova fattispecie è stata inserita dall'art.3 l.n.186/2014 al fine di superare, anche in ottemperanza ad indicazioni di fonte internazionale, uno dei principali ostacoli all'effettiva applicazione delle

fattispecie fin qui esaminate, rappresentato dal cd. privilegio dell'autoriciclaggio, per effetto del quale non era punibile a titolo di riciclaggio o impiego l'autore o il concorrente nel reato presupposto.

Anziché provvedere alla semplice eliminazione delle clausole espressive di tale "privilegio" dalle fattispecie degli artt. 648 bis e 648 ter, il legislatore ha inserito una fattispecie di nuovo conio, sanzionata meno severamente.

Il reato di autoriciclaggio si configura nel caso in cui chi abbia commesso o concorso a commettere un delitto non colposo impieghi, sostituisca o trasferisca in attività economiche, finanziarie, industriali o speculative il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione dell'origine delittuosa. .

L'autoriciclaggio consiste, pertanto, nell'attività di occultamento dei proventi derivanti da crimini propri.

Non sono punibili le condotte per effetto delle quali i proventi illeciti sono destinati alla mera utilizzazione o al godimento personale.

Reati presupposto dell'autoriciclaggio

Nell'ambito di attività d'impresa, pare possibile individuare taluni reati che più facilmente possono essere fonte di proventi illeciti per l'ente: così, ad esempio, i reati tributari, la truffa o la corruzione (anche tra privati).

È bene precisare che, ai fini della sussistenza della responsabilità dell'ente non si richiede che i proventi derivino da reati presupposto di una responsabilità dell'ente: il reato presupposto della responsabilità amministrativa dell'ente è infatti il reato di autoriciclaggio, non i reati presupposto di tale reato.

Può tuttavia essere opportuno – ai fini di una più efficace prevenzione del rischio di una responsabilità dell'ente nascente dalla commissione del reato di autoricicilaggio – prevedere nel Modello anche misure idonee a prevenire il rischio di commissione di altri reati, per quanto non compresi fra i reati "231" – laddove per tipologia e frequenza assumano significativa rilevanza.

Tale sembra essere il caso per i reati tributari e per il reato di truffa comune, per quanto, si ripete, tali reati, di per sé, non costituiscano reati “231”.

Si analizzeranno, quindi, brevemente tali tipologie di reato.

- **A) I REATI TRIBUTARI**

I reati tributari, previsti dal D. Lgs. 74/2000 recante la “nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell’art. 9 della legge 25 giugno 1999, n.205”, sono:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
- dichiarazione fraudolenta mediante artifici;
- dichiarazione infedele;
- omessa dichiarazione;
- emissione di fatture o di altri documenti per operazioni inesistenti;
- occultamento o distruzione di documenti contabili;
- omesso versamento di ritenute certificate;
- omesso versamento di IVA;
- indebita compensazione;
- sottrazione fraudolenta al pagamento di imposte.

- **B) REATI DI TRUFFA (EX ART. 640 C.P.)**

Il reato di truffa si configura ai sensi dell'art. 640 c.p. ogni volta che un qualsiasi soggetto, inducendo qualcuno in errore con artifizi o raggiri, procuri per sé o per altri un ingiusto profitto in danno di altri.

Il suddetto reato punisce le condotte aggressive contro il patrimonio personale altrui realizzate attraverso:

- artifizi, ossia attraverso una manipolazione o una trasfigurazione della realtà esterna, provocata mediante la simulazione di fatti o circostanze in realtà inesistenti o la dissimulazione di circostanze esistenti;
- raggiri, ossia attraverso un'attività simulatrice posta in essere con parole e argomentazioni che fanno scambiare il falso per il vero.

Si tenga conto che le suddette condotte devono essere idonee ad indurre in errore la vittima e pertanto non rilevano ai fini della configurazione del reato in esame artifizi o raggiri grossolani e palesemente non credibili.

In considerazione dell'attività svolta dalla Società, il suddetto reato assume particolare rilevanza nella forma della c.d. "truffa contrattuale", ossia in quell'elaborazione giurisprudenziale del reato di truffa ex art. 640 c.p. che è configurabile tutte le volte che in un rapporto contrattuale uno dei contraenti ponga in essere artifizi o raggiri diretti a tacere o a dissimulare fatti o circostanze tali che, ove conosciuti, avrebbero indotto l'altro contraente ad astenersi dal concludere il contratto.

In tali casi gli artifizi o i raggiri richiesti per la sussistenza del reato possono consistere anche nel silenzio maliziosamente serbato su alcune circostanze da parte di chi abbia il dovere di farle conoscere, indipendentemente dal fatto che dette circostanze potessero essere conoscibili dalla controparte con ordinaria diligenza.

Tali fattispecie, pertanto, sono particolarmente diffuse nelle relazioni contrattuali che, essendo connotate da un alto grado di asimmetria informativa, trovano specifica e dettagliata regolamentazione da parte delle Autorità di Vigilanza.

Le disposizioni regolamentari, infatti, prevedono in capo ai soggetti vigilati l'obbligo di comportarsi con diligenza e correttezza nell'interesse dei clienti operando in modo che essi siano adeguatamente informati e impongono agli stessi specifici obblighi giuridici di agire in modo tale da assicurare trasparenza ed equo apprezzamento delle condizioni contrattuali.

Brevi cenni sulla normativa in materia di prevenzione del riciclaggio (d.lgs.n.231/2007)

La normativa italiana in tema di prevenzione dei Reati di Riciclaggio prevede norme tese ad ostacolare le pratiche di riciclaggio, vietando tra l'altro l'effettuazione di operazioni di trasferimento di importi

rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati in appositi archivi.

Nello specifico, il corpo normativo in materia di riciclaggio è costituito anzitutto dal D. Lgs. 231/07 (Decreto Antiriciclaggio).

Il Decreto Antiriciclaggio – tra i cui destinatari figura la Società (vedi infra) – intende essenzialmente prevenire il rischio che il sistema finanziario sia utilizzato per il compimento di operazioni di riciclaggio e, a tal fine, pone a carico dei destinatari una serie di obblighi, il cui inadempimento è sanzionato, in alcuni casi, anche penalmente.

Proprio in considerazione della sua finalità preventiva, il d.lgs. n.231/2007 dà una definizione molto ampia della nozione di riciclaggio: tale definizione, per la quale si rinvia all'art.2 del decreto, ricomprende anche condotte che integrerebbero fattispecie di reato diverse dal riciclaggio, o che sarebbero prive di sanzione penale.

E' importante precisare che è alla nozione "amministrativa" di riciclaggio che la legge ricollega il sorgere di tutti gli obblighi di natura preventiva e degli obblighi di collaborazione attiva disciplinati dal decreto stesso.

Ai fini, invece, della responsabilità penale degli enti è necessario fare riferimento alle fattispecie di reato sopra esaminate, previste dal codice penale.

Non vi è dubbio, peraltro, che il puntuale rispetto di tutti gli obblighi imposti dal d.lgs.n.231/2007 sia indispensabile sotto il profilo della valutazione di adeguatezza del modello ai fini della prevenzione del rischio riciclaggio. Benché l'inadempimento degli obblighi "antiriciclaggio", anche nei casi in cui sia penalmente sanzionato, non sia idoneo a far sorgere una responsabilità dell'ente, in alcuni casi l'omesso rispetto degli obblighi "antiriciclaggio" (ad esempio, l'omessa segnalazione di operazione sospetta) potrebbe addirittura configurare, secondo talune pronunce giurisprudenziali, un concorso in una condotta di riciclaggio a carico dell'autore della violazione.

Il Decreto Antiriciclaggio prevede in sostanza i seguenti strumenti di contrasto del fenomeno del riciclaggio di proventi illeciti:

1. la previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiore a Euro 1.000. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.;

2. l'obbligo di adeguata verifica della clientela da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) in relazione ai rapporti ed alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi. In tale ambito rientra anche l'obbligo della clientela di fornire, sotto la propria responsabilità, tutte le informazioni necessarie ed aggiornate per consentire agli intermediari di adempiere agli obblighi di adeguata verifica;

3. l'obbligo di astenersi dall'apertura del rapporto continuativo, dall'esecuzione dell'operazione ovvero di porre fine al Rapporto Continuativo già in essere, qualora l'intermediario non sia in grado di rispettare gli obblighi di adeguata verifica della clientela;

4. l'obbligo da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) di conservare, nei limiti previsti dall'art. 36 del Decreto Antiriciclaggio, i documenti o le copie degli stessi e registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio, nonché autoriciclaggio, o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;

5. l'obbligo di segnalazione da parte di alcuni soggetti (elencati agli artt. 10, comma 2, 11, 12, 13 e 14 del Decreto Antiriciclaggio) all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio, nonché autoriciclaggio.

Sono sospette quelle operazioni che per caratteristiche, entità, natura o per qualsivoglia altra circostanza inducano a ritenere che il danaro, i beni e le utilità oggetto delle operazioni medesime possano provenire dalla commissione di reati in genere.

Si indicano quali possibili indici di anomalia (in considerazione della continua evoluzione delle modalità di svolgimento delle operazioni finanziarie, l'elenco è a titolo esemplificativo e non esaustivo):

a. ripetute operazioni della stessa natura non giustificate dall'attività svolta dal cliente ed effettuate con modalità tali da denotare intenti dissimulatori (es. accensione, da parte del medesimo contraente, di un elevato numero di polizze vita entro un determinato arco di tempo);
b. operazioni di ingente ammontare che risultano inusuali rispetto a quelle di norma effettuate dal cliente, soprattutto se non vi sono plausibili giustificazioni economiche o finanziarie;
c. ricorso a tecniche di frazionamento dell'operazione idonee ad eludere gli obblighi di identificazione e registrazione (ad es. per il pagamento delle rate di premio);
d. operazioni con configurazione illogica, soprattutto se risultano svantaggiose per il cliente sotto il profilo economico o finanziario (ad es. acquisto di polizze assicurative a valori non coerenti a quelli di mercato);
e. operazioni effettuate frequentemente da un cliente in nome o a favore di terzi, qualora i rapporti non appaiano giustificati (ad es. frequente stipula di polizze con beneficiari non appartenenti al nucleo familiare);
f. operazioni richieste con indicazioni palesemente inesatte o incomplete, tali da far ritenere l'intento di occultare informazioni essenziali, soprattutto se riguardanti i soggetti interessati all'operazione;
g. riscatto della polizza, nei casi di:
    1. esecuzione di riscatti totali effettuati con perdita pari o superiore al 20% tra premio versato e capitale lordo riscattato;
    2. effettuazione sulla stessa polizza più riscatti parziali per un importo inferiore a 5000 €;

h. ricorso al contante in sostituzione degli usuali mezzi di pagamento utilizzati dal cliente;

i. ricorso a tecniche di co-intestazione dei contratti aventi ad oggetto polizze assicurative ovvero variazioni delle intestazioni senza plausibili giustificazioni.

16.2 Attività Sensibili

La principale Attività Sensibile e le Attività strumentali, che APP Broker ha individuato al proprio interno come rilevante per la presente famiglia di reati sono le seguenti.

A) Gestione dei flussi monetari e finanziari

L'Attività Sensibile in questione riguarda la gestione dei flussi monetari e finanziari della Società, con specifico riferimento alla gestione delle entrate (incassi, disinvestimenti di liquidità, etc.) e delle uscite (investimenti della liquidità, acquisti, consulenze, etc.).

16.3 Principi generali di comportamento

I Destinatari devono attenersi – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento di attività nelle Aree a Rischio individuate in precedenza – a regole di condotta conformi a quanto prescritto nel presente Modello e nelle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati di Riciclaggio.
In particolare, i soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai Reati di Riciclaggio, finanziamento del terrorismo o con finalità di terrorismo o eversione dell'ordine democratico;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

- tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure aziendali interne in tutte le attività finalizzate alla gestione anagrafica di Fornitori;
- assicurare un'approfondita conoscenza dei soggetti terzi con i quali vengono instaurati rapporti nell'esercizio del business aziendale, ovvero beneficiari di atti di disposizione del patrimonio libero della Società;
- monitorare costantemente i flussi di denaro in uscita;
- non effettuare alcuna operazione che possa presentare carattere anomalo per tipologia o oggetto ovvero che possa determinare l'instaurazione o il mantenimento di rapporti che presentino profili di anomalia dal punto di vista dell'affidabilità e/o della reputazione delle controparti;
- non effettuare alcuna operazione – in via diretta o per il tramite di interposta persona – con soggetti, persone fisiche o giuridiche, residenti nella Lista Paesi predisposta dal Gruppo;
- non riconoscere compensi a favore di Consulenti e Fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi o che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alla prassi vigenti in ambito locale;
- non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- non selezionare personale in azienda i cui requisiti e la cui affidabilità non sia stata adeguatamente esaminata, compatibilmente con la legislazione vigente.

Al fine dell'efficace attuazione di quanto sopra riportato, la Società adotta procedure in applicazione delle quali:

- i dati raccolti relativamente ai rapporti con clienti, Consulenti risultino completi ed aggiornati, sia per la corretta e tempestiva individuazione dei medesimi sia per una valida valutazione del loro profilo;
- la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia.

16.4 Principi specifici per le procedure

Ai fini dell'attuazione delle regole elencate al precedente paragrafo 16.3, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali specifici qui di seguito descritti.
Inoltre, a presidio dei reati fonte dell'Autoriciclaggio, si considerino le disposizioni riportate nelle Parti Speciali e poste a mitigazione di tutte le fattispecie di Reato a cui la Società risulta esposta, con particolare riferimento ai Reati Societari e ai Reati di Criminalità Organizzata.

A) Gestione dei flussi monetari e finanziari

Al fine di scongiurare il pericolo di commissione dei reati previsti nella presente Parte Speciale, è necessario:

- che qualunque transazione finanziaria presupponga la conoscenza del beneficiario della relativa somma;
- avere sempre conoscenza dell'utilizzo che verrà fatto dei fondi della Società gestiti da terzi.

Al fine dell'efficace attuazione di quanto sopra riportato, i Dipendenti, gli Organi Societari (nonché i Consulenti nella misura necessaria alle funzioni dagli stessi svolte) operano in base a procedure che consentano quanto segue:

- i dati raccolti relativamente ai rapporti con Consulenti devono essere completi ed aggiornati, sia per la corretta e tempestiva individuazione dei medesimi sia per una valida valutazione del loro profilo;
- la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia;
- siano posti in essere controlli sulle attività di selezione delle Controparti Contrattuali, dei Dipendenti, dei Consulenti e dei Fornitori;
- utlilizzo del c/c di APP BROKER (conto Allianz Bank)

Si precisa che la tesoreria è gestita in outsourcing da Allianz S.p.A. per conto di APP Broker

CAPITOLO 17 – INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (art. 25 decies del Decreto)

17.1. La fattispecie del delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Il delitto di cui all'art. 377-bis del codice penale è stato inserito nel catalogo dei reati presupposto della L. 3 agosto 2009, n. 116 (art. 25-decies D.lgs. 231/2001)

Nello specifico, la disposizione del codice penale sanziona – salvo che il fatto costituisca reato più grave – «chiunque, 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 la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere».

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377 bis c.p.)

Tale reato è stato inserito in via prudenziale, si tratta del reato 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.

17.2. Attività sensibili

La principale Attività Sensibile, che APP Broker ha individuato al proprio interno come rilevante per la presente famiglia di reati, è la seguente:

A) Gestione del contenzioso: l'Attività Sensibile in questione riguarda la gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale, con particolare riferimento a:

- ogni ipotesi di indagine o di procedimento giudiziario penale riguardante o connesso con l'attività aziendale, anche a livello transnazionale;

- ogni ipotesi di indagine o di procedimento giudiziario penale riguardante o connesso con la prestazione di coperture assicurative o di garanzie fidejussorie aventi implicazioni transnazionali.

17.3. Principi Generali di Comportamento

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle Attività Sensibili rispetto al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria di cui all'art. 25-decies del D.Lgs. 231/2001.

In via generale, a tali soggetti è richiesto di:

- evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di polizia giudiziaria e dall'autorità giudiziaria inquirente e giudicante, fornendo tutte le informazioni, i dati e le notizie eventualmente utili;
- mantenere, nei confronti degli organi di polizia giudiziaria e dell'autorità giudiziaria un comportamento disponibile e collaborativo in qualsiasi situazione.

È fatto espresso divieto ai Destinatari, di ricorrere alla forza fisica, a minacce o all'intimidazione oppure promettere, offrire o concedere un'indebita utilità per indurre colui il quale può avvalersi della facoltà di non rispondere nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all'autorità giudiziaria, con l'intento di ottenere una pronuncia favorevole alla Società o determinare il conseguimento di altro genere di vantaggio.

È inoltre vietato:

- intrattenere rapporti con persone sottoposte alle indagini preliminari e imputati nel processo penale al fine di turbare la loro libertà di autodeterminazione;
- riconoscere forme di liberalità o altre utilità a dipendenti o terzi che siano persone sottoposte alle indagini preliminari e imputati nel processo penale per indurli a omettere dichiarazioni o a falsare le stesse, in favore della Società.

CAPITOLO 18 – IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (Art. 25 duodecies del Decreto)

18.1. Le fattispecie di reato di impiego di cittadini terzi il cui soggiorno è irregolare

Il delitto di "impiego di cittadini terzi il cui soggiorno è irregolare", previsto dall'art. 22, co. 12 *bis* D.Lgs. n. 286 del 1998, è stato introdotto nel novero dei c.d. "Reati Presupposto" del Decreto 231, all'articolo l'art. 25-duodecies, dal Decreto Legislativo 16 luglio 2012, n. 109, il quale, entrato in vigore il 9 agosto 2012, disciplina l'attuazione della Direttiva 2009/52/CE.

Sono inoltre trattati per analogia di presidi, nella presente Parte Speciale, i delitti contro "la personalità individuale", con specifico riferimento a quanto previsto dall'art. 603-bis del codice penale, ai sensi di quanto disposto dall'art. 12, comma 1, della Legge 29 ottobre 2016, n. 199, recante "Disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo", a decorrere dal 4 novembre 2016.

Di seguito si provvede a fornire una breve descrizione di tale delitto, in quanto ritenuto rilevante in via prudenziale in relazione all'attività svolta dalla Società (cfr. Matrice delle attività a rischio-reato).

- **Delitto di impiego di cittadini terzi il cui soggiorno è irregolare (art. 25-duodecies del D.Lgs. 231/2001)**

Tale reato si configura qualora il soggetto che riveste la qualifica di datore di lavoro occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o sia stato revocato o annullato, laddove i lavoratori occupati siano:

a) in numero superiore a tre;

b) minori in età non lavorativa;

c) sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui all'articolo 603-bis, c.p.

- **Delitti contro la personalità individuale (art. 25-quinquies del D.Lgs. 231/2001)**

Sebbene i reati della specie di cui all'art. 25-quinquies siano stati esclusi dalla trattazione del presente Modello, in quanto ritenuti non applicabili, se non in via remota, si richiamano limitatamente al cd. Reato di "Caporalato", di cui all'art. 603-bis del c.p..

Tale reato si configura quando chiunque:

a) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;

b) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

a) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;

b) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;

c) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;

d) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

18.2. Attività sensibili

La principale Attività Sensibile, che APP Broker ha individuato al proprio interno come rilevante per la presente famiglia di reati, è la seguente:

- **Assunzione e gestione di personale dipendente comunitario e/o extracomunitario**, in particolare con riferimento alle seguenti attività:
  - richiesta e verifica del permesso di soggiorno;
  - monitoraggio e rinnovo del permesso di soggiorno;
  - verifica dei limiti di età;
  - verifica delle condizioni di lavoro;
  - la verifica della regolarità contributiva;
  - il rispetto delle condizioni normative e retributive dei contratti collettivi di lavoro applicabili.

18.3. Principi Generali di Comportamento

I seguenti principi di carattere generale si applicano ai Dipendenti della Società in forza di apposite clausole contrattuali.

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi (anche internazionali) vigenti e applicabili alla realtà aziendale, nonché alle procedure ed ai regolamenti aziendali e di Gruppo e alle regole ed ai principi contenuti nel presente Modello.

Ai Destinatari sopra individuati è fatto in particolare divieto di:

- porre in essere comportamenti tali da integrare le fattispecie di reato richiamate dagli artt. 25-duodecies e 25-quinquies del Decreto 231;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé la fattispecie di reato qui considerata, possano potenzialmente diventarlo o favorirne la commissione.

A tal fine la Società:

- considera sempre prevalente la tutela dei diritti delle persone e dei lavoratori rispetto a qualsiasi considerazione economica;
- vieta l'assunzione di dipendenti stranieri privi di permesso di soggiorno regolare e vieta di conferire incarichi ad appaltatori e/o subappaltatori che, al contrario, se ne avvalgano;
- assicura massima tracciabilità e trasparenza nella gestione dei rapporti con società che svolgono attività in appalto per conto della Società stessa;
- si attiene alle condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro applicabili;
- assicura la regolarità nei pagamenti e negli adempimenti previdenziali, assistenziali e assicurativi nonché in tutti gli altri obblighi previsti dalla normativa di riferimento.

18.4. Principi specifici per le procedure

Relativamente all'attività di assunzione e gestione di personale dipendente comunitario e/o extracomunitario si applicano i principi di seguito enunciati:

- si impegna ad ottemperare a tutti gli obblighi verso i dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro ed assicurazioni sociali, assumendo a suo carico tutti gli oneri relativi;
- si obbliga, altresì, ad applicare, nei confronti dei propri dipendenti, condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro applicabili alla categoria e nella località in cui si svolgono le prestazioni, nonché le condizioni risultanti da successive modifiche o integrazioni;
- si obbliga, inoltre, a continuare ad applicare i suindicati contratti collettivi di lavoro anche dopo la loro scadenza e fino alla loro sostituzione;
- in caso di assunzione di cittadini stranieri residenti in Paesi Extracomunitari, la Società si attiva presso le autorità competenti al fine di ottenere tutta la documentazione necessaria a

consentire l'ingresso legale in Italia del cittadino straniero e l'instaurazione di un rapporto di lavoro regolare;

- in caso di assunzione di cittadini stranieri già soggiornanti in Italia la Società verifica che i medesimi siano in possesso di un permesso di soggiorno regolare o che in caso di scadenza dello stesso i medesimi abbiano provveduto ad avviare le pratiche per il rinnovo;
- la Società controlla che in occasione della scadenza dei permessi di soggiorno dei dipendenti stranieri, questi ultimi abbiamo provveduto ad avviare le relative pratiche di rinnovo, assicurando loro collaborazione nel rilascio della documentazione attestante l'impiego regolare presso la Società stessa;
- assicura che, qualora l'adempimento delle attività descritte ai punti precedenti avvenisse ricorrendo ai servizi di un'agenzia esterna specializzata, il rapporto con quest'ultima sia disciplinato da accordo scritto, il quale preveda – inter alia – l'obbligo dell'agenzia esterna a non porre in essere comportamenti che violino le disposizioni di cui al Decreto 231 e a rispettare, per quanto applicabile, il Modello della Società.

APPENDICE 1 – I REATI PREVISTI DAL DECRETO

Si elencano di seguito i reati attualmente ricompresi nell'ambito di applicazione del D.lgs. 231/2001, precisando tuttavia che si tratta di un elenco oggetto di periodiche integrazioni da parte del Legislatore:

1 Reati contro la Pubblica Amministrazione (artt. 24 e 25):

- Malversazione a danno dello Stato o di altro ente pubblico o dell'Unione Europea (art. 316 *bis* c.p.);
- Indebita percezione di erogazioni a danno dello Stato o di altro ente pubblico o dell'Unione Europea (art. 316 *ter* c.p.);
- Truffa in danno dello Stato o di un ente pubblico (art. 640, comma 2, n. 1, c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.);
- Frode informatica a danno dello Stato o di altro ente pubblico (art. 640 *ter* c.p.);
- Concussione (art. 317 c.p.);
- Corruzione (artt. 318, 319, 319 *bis*, 320, 321, 322 *bis* c.p.);
- Corruzione in atti giudiziari (art. 319 *ter* c.p.);
- Induzione indebita a dare o promettere utilità (art. 319 *quater* c.p.), come inserito dalla Legge 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- Istigazione alla corruzione (art. 322 c.p.);
- Traffico di influenze illecite (art. 346 bis c.p.).

2 Delitti informatici e trattamento illecito di dati, introdotti dalla Legge 48/2008 (art. 24-bis):

- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);

- Detenzione e 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.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
- 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.);
- Danneggiamento di sistemi informatici e telematici (art. 635- quater c.p.);
- Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).

3 <u>Delitti di criminalità organizzata, introdotti dalla Legge 94/2009 (art. 24 ter):</u>

- Associazione per delinquere, anche diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286 (art 416 c.p.);
- Associazioni di tipo mafioso anche straniere (art. 416-bis c.p.);
- Scambio elettorale politico-mafioso (art. 416-ter c.p.);
- Sequestro di persona a scopo di estorsione (art. 630 c.p.);

- Associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990 n. 309);
- Delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2 comma 3, della legge 18 aprile 1975, n. 110 (art. 407 comma 2, lett. a), numero 5) c.p.p.).

4 Reati transnazionali, introdotti dalla Legge 146/2006:

- Associazione per delinquere (art. 416 c.p.);
- Associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (DPR 43/1973, art. 29- *quater*);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (DPR 309/1990, art. 74);
- Disposizioni contro le immigrazioni clandestine (D.lgs. 286/1998, art. 12);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.);
- Favoreggiamento personale (art. 378 c.p.).
-

5 Reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, introdotti dalla Legge 409/2001 e modificati con Legge 99/2009 (art. 25-*bis*):

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);

- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Uso di valori bollati contraffatti o alterati (art. 464);
- Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (474 c.p.).

6 Delitti contro l'industria e il commercio, introdotti dalla Legge 99/2009 (art. 25-*bis* 1):

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.).

7 Reati societari, introdotti dal D.lgs. 61/2002 e modificati dalla Legge 262/2005 (art. 25-*ter*):

- False comunicazioni sociali (art. 2621 c.c.);
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629 *bis* c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.);
- Corruzione tra privati (art. 2635 c.c.) come inserito dalla Legge 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione".
- Istigazione alla corruzione tra privati (art. 2635-bis c.c.)

8 Delitti con finalità di terrorismo o di eversione dell'ordine democratico, introdotti dalla Legge 7/2003 (art. 25 *quater*):

- Associazioni sovversive (art. 270 c.p.);
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-*bis* c.p.);
- Assistenza agli associati (art. 270-*ter* c.p.);
- Arruolamento con finalità di terrorismo anche internazionale art. 270-*quater* c.p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinques* c.p.);
- Condotte con finalità di terrorismo (art. 270-*sexies* c.p.);
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.);
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280-*bis* c.p.);
- Attentato contro la costituzione dello Stato (art. 283 c.p.);
- Insurrezione armata contro i poteri dello Stato (art. 284 c.p.);
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289-*bis* c.p.);
- Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica (art. 1 D.L. 15/12/1979, n. 625 convertito con modifiche in L. 6/02/1980, n. 15);
- Convenzione internazionale per la repressione del finanziamento del terrorismo New York 9 dicembre 1999 (art. 2).

9 Pratiche di mutilazione degli organi genitali femminili, introdotti dalla Legge 7/2006 (art. 25–*quater.* 1)

10 Delitti contro la personalità individuale, introdotti dalla Legge 228/2003 e modificati con la Legge 38/2006 e con il D.lgs. 39/2014 (art. 25 *quinquies*):

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600-*bis*, commi 1 e 2, c.p.);

- Pornografia minorile (art. 600-*ter* c.p.);
- Detenzione di materiale pornografico (art. 600-*quater* c.p.);
- Pornografia virtuale (art. 600-*quater*.1 c.p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.);
- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.);
- Adescamento di minorenni (art. 609-*undecies* c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)

11 Abusi di mercato, introdotti dalla Legge 62/2005 e modificati dalla Legge 262/2005 (art. 25-*sexies*):

- Abuso di informazioni privilegiate (art. 184 D.lgs. 58/1998);
- Manipolazione del mercato (art. 185 D.lgs. 58/1998).

12 Reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro, introdotti dalla Legge 123/2007 (art. 25-*septies*):

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose, gravi o gravissime (art. 590 c.p.).

13 Reati in materia di ricettazione, riciclaggio e impiego di denaro di provenienza illecita, nonché di autoriciclaggio, introdotti dal D.lgs. 231/2007 (art. 25-*octies*):

- 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.);

- Autoriciclaggio (art. 648 *ter* 1 c.p.)

14 Delitti in materia di violazione del diritto d'autore, introdotti dalla Legge 99/2009 (art. 25-*novies*):

- Immissione su sistemi di reti telematiche, a disposizione del pubblico, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa (art. 171 comma 1, lett. a-*bis*), Legge 633/1941);
- Reati di cui al punto precedente commessi in riferimento ad un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore (art. 171, comma 3, Legge 633/1941);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi intesi unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori (art. 171-*bis*, comma 1, Legge 633/1941);
- Riproduzione, trasferimenti su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-*quinquies* e 64-*sexies* Legge 633/1941, al fine di trarne profitto e su supporti non contrassegnati SIAE; estrazione o reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-*bis* e 102-*ter* Legge 633/41; distribuzione, vendita e concessione in locazione della banca di dati (art. 171-*bis*, comma 2, Legge 633/1941);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi nastri o

supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento, di opere, o parti di opere, letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; detenzione per la vendita o la distribuzione, messa in commercio, concessione in noleggio o comunque cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo della televisione con qualsiasi procedimento, trasmissione a mezzo della radio, ascolto in pubblico delle duplicazioni o riproduzioni abusive menzionate; detenzione per la vendita o la distribuzione, messa in commercio, vendita, noleggio, cessione a qualsiasi titolo, trasmissione a mezzo della radio o della televisione con qualsiasi procedimento, di videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o di altro supporto per il quale è prescritta, ai sensi della Legge 633/1941, l'apposizione di contrassegno SIAE, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; ritrasmissione o diffusione con qualsiasi mezzo, in assenza di accordo con il legittimo distributore, di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato; introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, distribuzione, vendita, concessione in noleggio, cessione a qualsiasi titolo, promozione commerciale, installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto; fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicizzazione per la vendita o il noleggio, o detenzione per scopi commerciali, di attrezzature, prodotti o componenti, ovvero prestazione di servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all' art. 102-*quater,* Legge 633/1941 ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure; rimozione abusiva o alterazione delle informazioni elettroniche di

cui all'articolo 102-*quinquies*, ovvero distribuzione, importazione a fini di distribuzione, diffusione per radio o per televisione, comunicazione o messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse (art. 171-*ter* comma 1, Legge 633/1941);

- Riproduzione, duplicazione, trasmissione o abusiva diffusione, vendita o messa in commercio, cessione a qualsiasi titolo o abusiva importazione di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; comunicazione al pubblico, a fini di lucro, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; commissione di uno dei reati di cui al punto precedente esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi; promozione o organizzazione delle attività illecite di cui al punto precedente (art. 171-*ter* comma 2, Legge 633/1941);
- Mancata comunicazione alla SIAE, da parte di produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-*bis* Legge 633/1941, entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione, dei dati necessari alla univoca identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione sull'assolvimento degli obblighi di cui all'art. 181*bis*, comma 2 di detti dati (art. 171-*septies,* Legge 633/1941);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzazione per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-*octies,* Legge 633/1941).

15 Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, introdotto dalla Legge 116/2009 (art. 25-*decies*):

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

16 Reati ambientali, introdotti dal D. Lgs. 121/2011 (art. 25-*undecies*):

- Inquinamento ambientale (452 bis c.p.);
- Disastro ambientale (452 quater c.p.);
- Delitti colposi contro l'ambiente (452 quinquies c.p.);
- Traffico e abbandono di materiale ad alta radioattività (452 sexies c.p.);
- Circostanze aggravanti (452 octies c.p.);
- Attività organizzate per il traffico illecito di rifiuti (452 quaterdecies c.p.);
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 bis c.p.);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 bis c.p.);
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. 150/1992, art. 1, art. 2, art. 3 bis e art. 6);
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D.Lgs n.152/2006, art. 137);
- Attività di gestione di rifiuti non autorizzata (D.Lgs 152/2006, art. 256);
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D.Lgs 152/2006, art. 257);
- Traffico illecito di rifiuti (D.Lgs n.152/2006, art. 259);

- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.Lgs 152/2006, art. 258);
- Superamento di valori limite di emissione che determinano il superamento dei valori limite di qualità dell'aria (D.Lgs. 152/2006, art. 279);
- Inquinamento doloso provocato da navi (D.Lgs. 202/2007, art. 8);
- Inquinamento colposo provocato da navi (D.Lgs. 202/2007, art. 9);
- Cessazione e riduzione dell´impiego delle sostanze lesive (L. 549/1993 art. 3).

17 Reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, introdotto nel Decreto dal D. Lgs. 109/2012 (art. 25-*duodecies*):

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 commi 12 e 12-*bis* del D. Lgs. n. 286/1998).

18 Reato di Razzismo e xenofobia, introdotto nel Decreto dalla L.167/2017 (art. 25 *terdecies*):

- Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (art. 640-bis c.p.).

19 Frodi sportive, introdotto nel Decreto dalla L. 39/2019 (Art. 25-*quaterdecies*):

- Frode in competizione sportive (art. 1 Legge 401/1989);
- Esercizio abusivo di attività di giuoco o di scommessa (art. 4 Legge 401/1989).