



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

INDICE

CAPITOLO 1	IL CONTESTO NORMATIVO.....	6
1.1	Il regime di responsabilità amministrativa previsto dal decreto legislativo 8 giugno 2001, n. 231 a carico delle persone giuridiche, società ed associazioni anche prive di personalità giuridica.....	6
1.2	L'adozione dei modelli di organizzazione, gestione e controllo quali esimenti della responsabilità amministrativa dell'Ente.....	7
CAPITOLO 2	IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 DI ANTI FINANCIAL CRIME DIGITAL HUB S.C.A.R.L.	9
2.1	Gli strumenti aziendali esistenti quali presupposti del Modello	9
2.1.1.	<i>Premessa.....</i>	9
2.1.2.	<i>Codice Etico, Codice Interno di Comportamento di Gruppo e Linee Guida Anticorruzione di Gruppo.....</i>	11
2.1.3.	<i>Le caratteristiche salienti del sistema dei controlli interni.....</i>	11
2.1.4.	<i>Il sistema dei poteri e delle deleghe</i>	12
2.2	Le finalità perseguite con l'adozione del Modello.....	13
2.3	Gli elementi fondamentali del Modello	13
2.4	La Struttura del Modello	14
2.5	I destinatari del Modello.....	16
2.6	Adozione, efficace attuazione e modificazione del Modello – Ruoli e responsabilità .	16
2.6.1	<i>Direttore Generale</i>	17
2.6.2	<i>Funzione Compliance della Capogruppo</i>	17
2.6.3	<i>Funzione Internal Auditing della Capogruppo</i>	18
2.6.4	<i>Funzione Gestione Service Segreterie Controllate della Capogruppo.....</i>	18
2.6.5	<i>Funzione Legale e Contenzioso della Capogruppo.....</i>	18
2.6.6	<i>Funzione M&A e Partecipazioni della Capogruppo</i>	19
2.6.7	<i>Funzione Personale della Capogruppo</i>	19
2.6.8	<i>Datore di Lavoro e Committente ai sensi del D. Lgs. 81/2008 e Responsabile ambientale ai sensi del D. Lgs. 152/2006</i>	19
2.6.9	<i>Unità Organizzative della Società</i>	20
2.7	Attività oggetto di esternalizzazione.....	20
2.8	Il ruolo della Capogruppo	21
2.8.1	<i>Principi di indirizzo di Gruppo in materia di Responsabilità amministrativa degli Enti</i>	21
CAPITOLO 3	L'ORGANISMO DI VIGILANZA (ODV)	24
3.1	Individuazione dell'Organismo di Vigilanza	24
3.2	Composizione, durata, funzionamento e compensi dell'Organismo di Vigilanza.....	24
3.3	Requisiti di eleggibilità, cause di decadenza e sospensione.....	25
3.3.1	<i>Requisiti di professionalità, onorabilità ed indipendenza</i>	25
3.3.2	<i>Verifica dei requisiti.....</i>	26
3.3.3	<i>Cause di decadenza</i>	26

3.3.4 Cause di sospensione, temporaneo impedimento e revoca	26
3.4 Compiti dell'Organismo di Vigilanza.....	27
3.5 Modalità e periodicità di riporto agli Organi Societari	29
CAPITOLO 4 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA	30
4.1 Flussi informativi da effettuarsi al verificarsi di particolari eventi ed in caso di segnalazioni whistleblowing.....	30
4.2 Flussi informativi periodici.....	32
4.2.1 Flussi informativi provenienti dalle Unità Organizzative.....	32
4.2.2 Flussi informativi da parte della Funzione Compliance della Capogruppo.....	32
4.2.3 Flussi informativi da parte della funzione Internal Auditing della Capogruppo.....	33
4.2.4 Flussi informativi da parte del Datore di lavoro ai sensi del D. Lgs. 81/2008.....	33
4.2.5 Flussi informativi da parte del Committente ai sensi del D. Lgs. 81/2008.....	33
4.2.6 Flussi informativi da parte del Responsabile Ambientale	33
4.2.7 Flussi informativi da parte della Funzione Personale della Capogruppo	34
4.2.8 Flussi informativi da parte del Direttore Generale	34
CAPITOLO 5 IL SISTEMA SANZIONATORIO	35
5.1 Il sistema sanzionatorio.....	35
5.1.1 Principi generali	35
5.1.2 Personale dipendente eventualmente assunto da AFC Digital HUB appartenente alle aree professionali e ai quadri direttivi	36
5.1.3 Personale dirigente.....	37
5.1.4 Personale dipendente distaccato dalla Capogruppo e/o da altre società del Gruppo.....	38
5.1.5 Soggetti esterni.....	38
5.1.6 Componenti del Consiglio di Amministrazione e Sindaco Unico.....	38
CAPITOLO 6 COMUNICAZIONE INTERNA E FORMAZIONE.....	39
6.1 Comunicazione interna.....	39
6.2 Formazione.....	40
CAPITOLO 7 GLI ILLECITI PRESUPPOSTO – AREE, ATTIVITÀ E RELATIVI PRINCIPI DI COMPORTAMENTO E DI CONTROLLO.....	42
7.1 Individuazione delle aree sensibili.....	42
7.2 Area sensibile concernente i reati contro la Pubblica Amministrazione e il reato di corruzione tra privati	44
7.2.1 Fattispecie di reato	44
7.2.2 Attività aziendali sensibili	51
7.2.2.1 Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione	53
7.2.2.2 Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione	59
7.2.2.3 Gestione dei finanziamenti pubblici.....	63
7.2.2.4 Gestione dei contenziosi e degli accordi transattivi	67
7.2.2.5 Gestione dei rapporti con le Autorità di Vigilanza.....	72

7.2.2.6	Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali	76
7.2.2.7	Gestione di omaggi, spese di rappresentanza e sponsorizzazioni	81
7.2.2.8	Gestione del processo di selezione e assunzione del personale.....	86
7.2.2.9	Gestione dei rapporti con i Regolatori	89
7.3	Area sensibile concernente i reati societari	93
7.3.1	<i>Fattispecie di reato</i>	93
7.3.2	<i>Attività aziendali sensibili</i>	98
7.3.2.1	Gestione dei rapporti con il Sindaco Unico e con la Società di Revisione	99
7.3.2.2	Gestione dell'informativa periodica	102
7.3.2.3	Acquisto, gestione e cessione di partecipazioni e di altri <i>asset</i>	106
7.4	Area sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali, i reati contro la persona e i reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa	110
7.4.1	<i>Fattispecie di reato</i>	110
7.4.2	<i>Attività aziendali sensibili</i>	117
7.5	Area sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio.....	119
7.5.1	<i>Fattispecie di reato</i>	119
7.5.2	<i>Attività aziendali sensibili</i>	123
7.5.2.1	Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose	124
7.6	Area sensibile concernente i reati in tema di salute e sicurezza sul lavoro.....	127
7.6.1	<i>Fattispecie di reato</i>	127
7.6.2	<i>Attività aziendali sensibili</i>	128
7.6.2.1	Gestione dei rischi in materia di salute e sicurezza sul lavoro.....	129
7.7	Area sensibile concernente i reati informatici e di indebito utilizzo di strumenti di pagamento diversi dai contanti	141
7.7.1	<i>Fattispecie di reato</i>	141
7.7.2	<i>Attività aziendali sensibili</i>	148
7.7.2.1	Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo .	150
7.7.2.2	Gestione e utilizzo degli strumenti di pagamento diversi dai contanti	159
7.8	Area sensibile concernente i reati contro l'industria e il commercio, i reati in materia di violazione del diritto d'autore e i reati doganali.....	162
7.8.1	<i>Fattispecie di reato</i>	162
7.8.2	<i>Attività aziendali sensibili</i>	168
7.9	Area sensibile concernente i reati ambientali	170
7.9.1	<i>Fattispecie di reato</i>	170
7.9.2	<i>Attività aziendali sensibili</i>	173
7.9.2.1	Gestione dei rischi in materia ambientale.....	175
7.10	Area sensibile concernente i reati tributari	179

7.10.1	<i>Fattispecie di reato</i>	179
7.10.2	<i>Attività aziendali sensibili</i>	181
7.10.2.1.	Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari.	183

CAPITOLO 1 IL CONTESTO NORMATIVO

1.1 Il regime di responsabilità amministrativa previsto dal decreto legislativo 8 giugno 2001, n. 231 a carico delle persone giuridiche, società ed associazioni anche prive di personalità giuridica

In attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, in data 8 giugno 2001 è stato emanato il Decreto Legislativo n. 231 (di seguito denominato il "Decreto" o anche "D. Lgs. 231/2001"), con il quale il Legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche. In particolare, si tratta della Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, della Convenzione firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale siano coinvolti funzionari della Comunità Europea o degli Stati membri e della Convenzione dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali. Il Decreto, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa a carico degli Enti (da intendersi come società, associazioni, consorzi, ecc., di seguito denominati "Enti") per reati tassativamente elencati e commessi¹ nel loro interesse o vantaggio: (i) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi, ovvero (ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

Il catalogo degli "illeciti presupposto" si è dilatato in tempi recenti con l'introduzione, nell'ambito degli illeciti presupposto, anche di alcune fattispecie di illecito amministrativo.

La responsabilità dell'Ente si aggiunge a quella della persona fisica, che ha commesso materialmente l'illecito, ed è autonoma rispetto ad essa, sussistendo anche quando l'autore del reato non è stato identificato o non è imputabile oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

La previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti ivi espressamente previsti, gli Enti che abbiano tratto vantaggio dalla commissione del reato o nel cui interesse siano stati compiuti i reati - o gli illeciti amministrativi - presupposto di cui al Decreto medesimo. A carico dell'Ente sono irrogabili sanzioni pecuniarie e interdittive, nonché la confisca, la pubblicazione della sentenza di condanna ed il commissariamento. Le misure interdittive, che possono comportare per l'Ente conseguenze più gravose rispetto alle sanzioni pecuniarie, consistono nella sospensione o revoca di licenze e concessioni, nel divieto di contrarre con la pubblica amministrazione, nell'interdizione dall'esercizio dell'attività, nell'esclusione o revoca di finanziamenti e contributi, nel divieto di pubblicizzare beni e servizi.

¹ La responsabilità dell'ente sussiste anche nel caso di delitti tentati, ovvero nel caso in cui siano posti in essere atti idonei diretti in modo univoco alla commissione di uno dei delitti indicati come presupposto dell'illecito della persona giuridica.

La suddetta responsabilità si configura anche in relazione a reati commessi all'estero, purché per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi e l'Ente abbia nel territorio dello Stato italiano la sede principale.

1.2 L'adozione dei modelli di organizzazione, gestione e controllo quali esimenti della responsabilità amministrativa dell'Ente

Istituita la responsabilità amministrativa degli Enti, l'art. 6 del Decreto stabilisce che l'Ente non risponde nel caso in cui provi che il proprio organo dirigente abbia “...*adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi...*”.

La medesima norma prevede, inoltre, l'istituzione di un organismo di controllo interno all'Ente con il compito “...*di vigilare sul funzionamento e l'osservanza dei modelli...*”, nonché di curarne l'aggiornamento.

Il Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231 (di seguito denominato anche “Modello”) deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;
- prevedere specifici protocolli 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 di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Ove il reato venga commesso da soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che:

- a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento è stato affidato a un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo;
- c) i soggetti hanno commesso il reato eludendo fraudolentemente il Modello;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'Ente, prima della commissione del reato, abbia adottato ed efficacemente attuato

un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi, secondo una valutazione che deve necessariamente essere a priori.

L'art. 6 del Decreto dispone, infine, che il Modello possa essere adottato sulla base di codici di comportamento redatti da associazioni rappresentative di categoria e comunicati al Ministero della Giustizia.

Si precisa che il Modello di Anti Financial Crime Digital Hub S.c.a.r.l. (di seguito, anche "AFC Digital HUB" o "Società") è stato predisposto attenendosi – nel rispetto delle peculiarità dell'attività della Società e della sua struttura organizzativa – ai principi ed ai contenuti del Modello della Capogruppo Intesa Sanpaolo S.p.A. (di seguito anche la "Capogruppo" e/o "Intesa Sanpaolo") alle Linee Guida redatte dall'ABI, approvate dal Ministero della Giustizia.

CAPITOLO 2 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 DI ANTI FINANCIAL CRIME DIGITAL HUB S.C.A.R.L.

2.1 Gli strumenti aziendali esistenti quali presupposti del Modello

2.1.1. Premessa

Anti Financial Crime Digital Hub S.c.a.r.l. è una società consortile, senza scopo di lucro, a responsabilità limitata, del Gruppo Intesa Sanpaolo (di seguito anche il “Gruppo”), costituita in data 16 giugno 2022.

La Società ha per oggetto, in via prevalente, l’attività - nei confronti e/o nell’interesse dei soci - di ricerca, sviluppo e ingegnerizzazione di modelli di intelligenza artificiale volti al contrasto del crimine finanziario anche attraverso lo sviluppo di *partnership* con aziende, istituti finanziari, enti e istituzioni operanti nel settore della tecnologia, dell’innovazione digitale e dell’*anti financial crime*.

La Società può pubblicare i risultati delle ricerche svolte e provvedere alla ingegnerizzazione, ovvero trasformazione dei modelli sviluppati in *software* funzionanti e pronti per essere rilasciati in un contesto industriale.

Altresì, per facilitare la condivisione di soluzioni innovative, AFC Digital HUB può promuovere e organizzare programmi di formazione, seminari e conferenze, oltre che redigere *report* scientifici indirizzati anche ai *policymakers* e ai principali *stakeholders* del settore.

Sono stati nominati dal Consiglio di Amministrazione:

- uno Steering Committee, quale comitato tecnico-manageriale avente funzioni propositive, consultive ed istruttorie, nonché il compito di supportare l’organo amministrativo nel governo e coordinamento delle iniziative di ricerca, sviluppo e ingegnerizzazione dei modelli di intelligenza artificiale volti al contrasto del crimine finanziario;
- uno Scientific Advisory Board avente funzioni propositive e consultive in tema di indirizzo delle attività di ricerca e di formazione della Società.

La Società riceve i servizi necessari per lo svolgimento della propria attività, quando non coperti dalle proprie Unità Organizzative, dalla Capogruppo, in virtù di un apposito contratto di servizio in essere tra le parti.

Nella predisposizione del presente Modello si è tenuto innanzitutto conto della normativa, delle procedure e dei sistemi di controllo esistenti e già operanti in AFC Digital HUB, in quanto idonei a valere anche come misure di prevenzione di reati e di comportamenti illeciti in genere, inclusi quelli previsti dal D. Lgs. 231/2001.

Gli Organi Sociali di AFC Digital HUB hanno dedicato e continuano a dedicare la massima cura nella definizione in chiave unitaria delle strutture organizzative e delle procedure operative sia al fine di assicurare efficienza, efficacia e trasparenza nella gestione delle attività e nell’attribuzione delle correlate responsabilità, sia allo scopo di ridurre al minimo disfunzioni, malfunzionamenti ed irregolarità (tra i quali si annoverano anche comportamenti illeciti o comunque non in linea con quanto indicato dalla Società).

Il contesto organizzativo di AFC Digital HUB è costituito dall'insieme di regole, strutture e procedure che ne garantiscono il funzionamento della Società; si tratta dunque di un sistema estremamente articolato che viene definito e verificato internamente anche al fine di rispettare le previsioni normative e regolamentari a cui AFC Digital HUB è sottoposta anche in considerazione dell'appartenenza al Gruppo Intesa Sanpaolo.

AFC Digital HUB appartiene, come sopra indicato, al Gruppo Intesa Sanpaolo ed è soggetta – pertanto - all'attività di indirizzo, direzione, governo e coordinamento della Capogruppo. In tale qualità essa è tenuta ad osservare le disposizioni che la Capogruppo emana nel quadro delle attività di governo delle proprie controllate e partecipate.

Tra le previsioni normative rientra anche l'obbligo per la Capogruppo di redigere, ai sensi del D. Lgs. 254/2016, la Dichiarazione consolidata di carattere non finanziario che, nella misura necessaria ad assicurare la comprensione dell'attività del Gruppo, del suo andamento, dei suoi risultati e dell'impatto dalla stessa prodotta, copre i temi ambientali, sociali, attinenti al personale, al rispetto dei diritti umani, alla lotta contro la corruzione attiva e passiva. La Dichiarazione deve descrivere il modello aziendale di gestione ed organizzazione delle attività di impresa, ivi inclusi i modelli di organizzazione e di gestione adottati ai sensi del D. Lgs. 231/2001, le politiche praticate con riferimento alla gestione dei suddetti temi e dei principali rischi inerenti.

È dunque evidente che tale complesso di norme e disposizioni, costituiscono anche un prezioso strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli Enti.

Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali e ad effettuare i controlli sull'attività di impresa, anche in relazione ai reati e agli illeciti da prevenire, la Società ha individuato ed approvato:

- le regole di *corporate governance* adottate in recepimento della normativa societaria e regolamentare rilevante, nonché delle direttive emanate dalla Capogruppo;
- la normativa di Gruppo applicabile e recepita dalla Società;
- i regolamenti interni e le policy aziendali;
- il Codice Etico, il Codice Interno di Comportamento di Gruppo e le Linee Guida Anticorruzione di Gruppo;
- il sistema dei controlli interni;
- il sistema dei poteri e delle deleghe.

Le regole, le procedure e i principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello ma fanno parte del più ampio sistema di organizzazione, gestione e controllo che lo stesso intende integrare e che tutti i soggetti destinatari, sia interni che esterni, sono tenuti a rispettare, in relazione al tipo di rapporto in essere con la Società.

Nei paragrafi che seguono si intendono illustrare, per grandi linee, esclusivamente i principi di riferimento del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo, il sistema dei controlli interni, nonché il sistema dei poteri e delle deleghe.

2.1.2. Codice Etico, Codice Interno di Comportamento di Gruppo e Linee Guida Anticorruzione di Gruppo

A conferma dell'importanza attribuita ai profili etici ed a coerenti comportamenti improntati a rigore e integrità, AFC Digital HUB recepisce il Codice Etico, il Codice Interno di Comportamento di Gruppo e le Linee Guida Anticorruzione di Gruppo adottati da Intesa Sanpaolo S.p.A.

Il Codice Etico è uno strumento di autoregolamentazione volontaria, parte integrante del modello di gestione della Sostenibilità. Contiene la mission, i valori aziendali e i principi che regolano le relazioni con gli *stakeholder*, a partire dall'identità aziendale. In alcuni ambiti di particolare rilevanza (es. diritti umani, tutela del lavoro, salvaguardia dell'ambiente, lotta alla corruzione) richiama regole e principi coerenti ai migliori standard internazionali.

Il Codice Interno di Comportamento di Gruppo, applicabile a tutte le società del Gruppo, è costituito da un insieme, volutamente snello, di regole sia di carattere generale – che definiscono le norme essenziali di comportamento degli esponenti aziendali, di tutti i dipendenti e dei collaboratori esterni che, nell'ambito delle loro funzioni, sono tenuti ad esercitare le loro attività con professionalità, diligenza, onestà e correttezza – sia di carattere più specifico, ad esempio laddove si vietano determinate operazioni personali.

Le Linee Guida Anticorruzione di Gruppo in linea con le migliori prassi internazionali individuano i principi, identificano le aree sensibili e definiscono i ruoli, le responsabilità e i macro-processi per la gestione del rischio di corruzione da parte del Gruppo Intesa Sanpaolo.

Per le Società per le quali il presidio della conformità in materia di responsabilità amministrativa degli Enti è accentrato nella Capogruppo è prevista l'assegnazione alla Direzione Centrale Anti Financial Crime della Capogruppo della responsabilità di presidio della materia. Il ruolo di Responsabile Aziendale Anticorruzione viene identificato all'interno della predetta Direzione.

2.1.3. Le caratteristiche salienti del sistema dei controlli interni

AFC Digital HUB, per garantire una sana e prudente gestione, coniuga l'oggetto consortile con un'assunzione dei rischi consapevole e con una condotta operativa improntata a criteri di correttezza.

Pertanto, la Società, anche in coerenza con le Linee Guida fornite dalla Capogruppo, si è dotata di un sistema dei controlli interni idoneo a rilevare, misurare e verificare nel continuo i rischi tipici dell'attività sociale, ivi compresa quella svolta in *outsourcing*.

Il sistema dei controlli interni di AFC Digital HUB è costituito da linee guida, regole, processi, procedure e strutture organizzative che mirano ad assicurare il rispetto delle strategie aziendali e il conseguimento delle seguenti finalità:

- efficacia ed efficienza dei processi aziendali;
- salvaguardia del valore delle attività e protezione dalle perdite;
- affidabilità e integrità delle informazioni contabili e gestionali;
- conformità delle operazioni con la legge e con l'infrastruttura documentale della Società, ossia con l'insieme di politiche, piani, regolamenti e procedure interne, ivi compresa la documentazione emanata dalla Capogruppo e recepita, ove applicabile, dalla Società.

Il sistema dei controlli interni è delineato da un'infrastruttura documentale (l'"impianto normativo" adottato) che permette di ripercorrere in modo organico e codificato le linee guida, le procedure, le strutture organizzative, i rischi e i controlli applicabili, recependo, oltre agli indirizzi di Gruppo e aziendali, anche le disposizioni di Legge, ivi compresi i principi dettati dal D. Lgs. 231/2001.

L'impianto normativo è costituito da "Documenti di *Governance*", tempo per tempo adottati, che sovrintendono al funzionamento della Società (Statuto; Codice Etico, Codice Interno di Comportamento di Gruppo; Regolamento delle operazioni con parti correlate, Regolamento del sistema dei controlli interni integrato; Linee Guida Facoltà e poteri, Funzionigrammi delle strutture organizzative etc.) e da norme più strettamente operative che regolamentano i processi aziendali, le singole attività e i relativi controlli (Regole e Guide Operative etc.).

L'insieme degli elementi che costituiscono il sistema dei controlli interni disegna soluzioni organizzative volte a:

- assicurare una sufficiente separatezza tra le funzioni operative e quelle di controllo ed evitare situazioni di conflitto di interesse nell'assegnazione delle competenze;
- identificare, misurare e monitorare adeguatamente i principali rischi assunti nei diversi segmenti operativi;
- consentire la registrazione dei fatti di gestione e delle operazioni con adeguato grado di dettaglio, assicurandone la corretta attribuzione sotto il profilo temporale;
- assicurare sistemi informativi affidabili e idonee procedure di *reporting* ai diversi livelli direzionali ai quali sono attribuite funzioni di controllo;
- garantire che le anomalie riscontrate dalle unità operative, dalla Funzione Internal Auditing della Capogruppo o dalle altre ivi incluse quelle a cui sono attribuite funzioni di controllo, siano tempestivamente portate a conoscenza di livelli appropriati dell'azienda e gestite con immediatezza.

Inoltre, sono previste attività di controllo a ogni livello operativo che consentono l'univoca e formalizzata individuazione delle responsabilità, in particolare nei compiti di controllo e di correzione delle irregolarità riscontrate.

Il sistema dei controlli interni è periodicamente soggetto a ricognizione e adeguamento in relazione all'evoluzione dell'operatività aziendale e al contesto di riferimento.

2.1.4. Il sistema dei poteri e delle deleghe

A norma dello Statuto, il Consiglio di Amministrazione è investito di tutti i poteri per l'ordinaria e straordinaria amministrazione e di disposizione della Società che non siano riservati inderogabilmente dalla legge o dallo Statuto medesimo alla competenza dei soci.

Il Consiglio di Amministrazione, nei limiti previsti dalla legge, ha delegato parte delle proprie attribuzioni al Presidente del Consiglio di Amministrazione e al Direttore Generale, fissandone i relativi poteri.

In particolare, al Presidente del Consiglio di Amministrazione e al Direttore Generale sono conferiti i poteri di rappresentanza di fronte a qualsiasi autorità e alla firma sociale.

Inoltre, al Direttore Generale sono attribuiti poteri deliberativi e di spesa da esercitarsi nel rispetto dei limiti di Statuto e nell'ambito delle strategie, degli indirizzi e dei piani espressi dal Consiglio di Amministrazione. Il Consiglio di Amministrazione può, inoltre, delegare poteri di rappresentanza, con la relativa facoltà di firma, a dipendenti o ad altri soggetti, determinandone limiti e modalità. La facoltà di subdelega viene esercitata attraverso un processo trasparente, sempre monitorato, graduato in funzione del ruolo e della posizione ricoperta dal "subdelegato", comunque prevedendo sempre l'obbligo di informativa alla funzione delegante.

Sono inoltre formalizzate le modalità di firma sociale per atti, contratti, documenti e corrispondenza, sia esterna che interna.

Tutte le Unità Organizzative operano sulla base della normativa interna della Società ovvero della Capogruppo che definisce ambiti di competenza e di responsabilità e regola le modalità di svolgimento dei processi aziendali.

2.2 Le finalità perseguite con l'adozione del Modello

Nonostante gli strumenti aziendali illustrati nei paragrafi precedenti risultino di per sé idonei anche a prevenire i reati contemplati dal Decreto, AFC Digital HUB ha ritenuto opportuno adottare uno specifico "Modello di organizzazione, gestione e controllo ai sensi del Decreto Legislativo 8 giugno 2001, n. 231", nella convinzione che ciò costituisca, oltre che un valido strumento di sensibilizzazione di tutti coloro che operano per conto della Società affinché tengano comportamenti corretti e lineari, anche un più efficace mezzo di prevenzione contro il rischio di commissione dei reati e degli illeciti amministrativi previsti dalla normativa di riferimento.

In particolare, attraverso l'adozione ed il costante aggiornamento del Modello, la Società si propone di perseguire le seguenti principali finalità:

- determinare, in tutti coloro che operano per conto della Società nell'ambito di "attività sensibili" (ovvero di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto), la consapevolezza di poter incorrere, in caso di violazione delle disposizioni impartite in materia, in conseguenze disciplinari e/o contrattuali, oltre che in sanzioni penali e amministrative irrogabili nei loro stessi confronti;
- ribadire che tali forme di comportamento illecito sono fortemente condannate, in quanto le stesse (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali la Società, in linea con la Capogruppo, intende attenersi nell'esercizio dell'attività aziendale;
- consentire alla Società, grazie ad un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente, al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello.

2.3 Gli elementi fondamentali del Modello

Gli elementi fondamentali sviluppati nella definizione del Modello possono essere così riassunti:

- individuazione delle aree di attività a rischio ovvero delle attività aziendali sensibili nel cui ambito potrebbero configurarsi le ipotesi di reato da sottoporre ad analisi e monitoraggio;
- gestione di processi operativi in grado di garantire:

- la separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
- una chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa;
- corrette modalità di svolgimento delle attività medesime;
- la tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali o informatici;
- processi decisionali legati a predefiniti criteri oggettivi (es.: selezione dei fornitori facendo riferimento ad apposito albo istituito presso la Capogruppo, esistenza di criteri oggettivi di valutazione e selezione del personale, ecc.);
- l'esistenza e la tracciabilità delle attività di controllo e supervisione compiute sulle transazioni aziendali;
- la presenza di meccanismi di sicurezza in grado di assicurare un'adeguata protezione/accesso fisico-logico ai dati e ai beni aziendali;
- emanazione di regole comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale;
- definizione delle responsabilità nell'adozione, modifica, attuazione e controllo del Modello stesso;
- identificazione dell'Organismo di Vigilanza e attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- definizione dei flussi informativi nei confronti dell'Organismo di Vigilanza;
- definizione e applicazione di disposizioni idonee a sanzionare il mancato rispetto delle misure indicate nel Modello;
- formazione degli esponenti e del personale e comunicazione interna in merito al contenuto del Decreto e del Modello ed agli obblighi che ne conseguono.

2.4 La Struttura del Modello

Nel definire il presente Modello, la Società ha adottato un approccio che ha consentito di utilizzare e integrare nel Modello stesso le regole e la normativa interna già esistenti sulla base della mappatura delle aree e attività sensibili effettuata in occasione dell'adozione del Modello.

Sono state identificate per ciascuna categoria di "illeciti presupposto", le aree aziendali "sensibili". Nell'ambito di ogni area sensibile sono state poi individuate le attività aziendali nello svolgimento delle quali è più verosimile il rischio della commissione di illeciti presupposto previsti dal Decreto (c.d. attività "sensibili"), codificando per ciascuna di dette attività, principi di comportamento e di controllo – diversificati in relazione allo specifico rischio-reato da prevenire – cui devono attenersi tutti coloro che vi operano.

In sede di predisposizione del Modello, l'individuazione di dette attività sensibili è avvenuta attraverso l'analisi dei processi aziendali al fine di consentire la piena applicazione del Modello con l'apparato organizzativo di AFC Digital HUB.

In tal modo, il Modello trova piena ed efficace attuazione nella realtà della Società attraverso il collegamento di ciascuna attività “sensibile” con le strutture aziendali tempo per tempo coinvolte e con la gestione dinamica dei processi e della relativa normativa interna di riferimento, che deve basarsi sui principi di comportamento e di controllo enunciati per ciascuna di dette attività.

L’approccio seguito consente di:

- valorizzare al meglio il patrimonio conoscitivo già esistente nella Società in termini di politiche, regole e normative interne che indirizzano e governano la formazione e l’attuazione delle decisioni in relazione agli illeciti da prevenire e, più in generale, la gestione dei rischi e l’effettuazione dei controlli;
- gestire con criteri univoci le regole operative aziendali, incluse quelle relative alle aree “sensibili”;
- rendere più agevole la costante implementazione e l’adeguamento tempestivo dei processi e dell’impianto normativo interni ai mutamenti della struttura organizzativa e dell’operatività aziendale, assicurando un elevato grado di “dinamicità” del Modello.

In AFC Digital HUB il presidio dei rischi rivenienti dal D. Lgs. 231/2001 è pertanto assicurato:

- dal presente documento (*“Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231”*);
- dall’impianto normativo – anche della Capogruppo, ove applicabile e recepito dalla Società – che ne costituisce parte integrante e sostanziale.

Il *“Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231”* delinea in particolare:

- il contesto normativo di riferimento;
- il ruolo e la responsabilità delle strutture (anche della Capogruppo operanti in base al contratto di servizio in essere) coinvolte nell’adozione, efficace attuazione e modificazione del Modello;
- gli specifici compiti e responsabilità dell’Organismo di Vigilanza;
- i flussi informativi verso l’Organismo di Vigilanza;
- il sistema sanzionatorio;
- le logiche formative;
- le aree “sensibili” in relazione alle fattispecie di illecito di cui al Decreto;
- le attività aziendali nell’ambito delle quali può verificarsi il rischio di commissione degli illeciti presupposto ed i principi di comportamento e le regole di controllo volti a prevenirli (attività “sensibili”).

L’impianto normativo della Società, come definito al paragrafo 2.1, regola l’operatività di AFC Digital HUB nelle aree/attività “sensibili” e costituisce a tutti gli effetti parte integrante del Modello. L’impianto normativo è contenuto e catalogato, con specifico riferimento a ogni attività sensibile, in un apposito *repository* documentale, diffuso all’interno di tutta la Società tramite la rete Intranet aziendale e costantemente aggiornato a cura delle funzioni competenti in coerenza con l’evolversi dell’operatività.

Pertanto, dall'associazione dei contenuti del Modello con l'impianto normativo aziendale è possibile individuare, per ciascuna delle attività "sensibile", specifici, puntuali e sempre aggiornati Protocolli che descrivono fasi di attività, strutture coinvolte, principi di controllo e di comportamento, regole operative di processo e che consentono di rendere verificabile e congrua ogni fase di attività.

2.5 I destinatari del Modello

Il Modello e le disposizioni ivi contenute e richiamate devono essere rispettate dagli esponenti aziendali e da tutto il personale della Società, compresi gli eventuali dipendenti direttamente assunti presso la Società nonché i dipendenti della Capogruppo o di altre società del Gruppo che operano presso AFC Digital HUB in regime di distacco (di seguito anche il "Personale") e, in particolare, da parte di coloro che si trovino a svolgere le attività sensibili.

La formazione degli esponenti e del Personale e l'informazione interna sul contenuto del Modello vengono costantemente assicurati con le modalità meglio descritte al successivo Capitolo 6.

Al fine di garantire l'efficace ed effettiva prevenzione dei reati, il Modello è destinato anche ai soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i *partner*, o altri soggetti) che, in forza di rapporti contrattuali, prestino la loro collaborazione alla Società per la realizzazione delle sue attività. Nei confronti dei medesimi il rispetto del Modello è garantito mediante l'apposizione di una clausola contrattuale che impegni il contraente ad attenersi ai principi del Modello della Società, del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo e a segnalare all'Organismo di Vigilanza ed al Responsabile Aziendale Anticorruzione eventuali notizie della commissione di illeciti o della violazione del Modello prevedendosi che la violazione degli impegni o eventuali condotte illecite poste in essere in occasione o comunque in relazione all'esecuzione degli incarichi costituiranno a tutti gli effetti grave inadempimento ai sensi dell'art. 1455 cod. civ. ai fini della risoluzione del contratto.

2.6 Adozione, efficace attuazione e modificazione del Modello – Ruoli e responsabilità

Adozione del Modello

L'adozione e l'efficace attuazione del "*Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231*" costituiscono, ai sensi dell'art. 6, comma I, lett. a) del Decreto, atti di competenza e di emanazione del Consiglio di Amministrazione che approva, mediante apposita delibera, il Modello sentito il parere dell'Organismo di Vigilanza.

A tal fine, il Direttore Generale sottopone ad approvazione del Consiglio di Amministrazione il Modello predisposto con il supporto delle strutture competenti della Società e della Capogruppo, ciascuna per gli ambiti di rispettiva pertinenza.

Efficace attuazione e modificazione del Modello

È cura del Consiglio di Amministrazione (o di soggetto da questi formalmente delegato) provvedere all'efficace attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per implementarlo o modificarlo. Per l'individuazione di tali azioni, l'Organo amministrativo si avvale del supporto dell'Organismo di Vigilanza.

Il Consiglio di Amministrazione delega le singole Unità Organizzative a dare attuazione ai contenuti del Modello ed a curare il costante aggiornamento e implementazione della normativa interna e dei processi aziendali, che costituiscono parte integrante del Modello, nel rispetto dei principi di controllo e di comportamento definiti in relazione ad ogni attività sensibile. L'efficace e concreta attuazione del Modello è garantita altresì:

- dall'Organismo di Vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalle singole Unità Organizzative nelle aree sensibili;
- dai responsabili delle varie Unità Organizzative della Società e/o delle funzioni della Capogruppo in relazione alle attività a rischio dalle stesse svolte.

Il Consiglio di Amministrazione deve inoltre garantire, anche attraverso l'intervento dell'Organismo di Vigilanza, l'aggiornamento delle aree sensibili e del Modello, in relazione alle esigenze di adeguamento che si rendono necessarie nel tempo.

Specifici ruoli e responsabilità nella gestione del Modello sono inoltre attribuiti alle unità/strutture/funzioni di seguito indicate, anche nel caso di attività svolte in *outsourcing* dalle funzioni della Capogruppo o di eventuali altre società del Gruppo Intesa Sanpaolo, nonché di *outsourcer* esterni.

2.6.1 Direttore Generale

Il Direttore Generale con il supporto della struttura Planning Governance e Controls della Società al fine di meglio presidiare la coerenza della struttura organizzativa e dei meccanismi di governance rispetto agli obiettivi perseguiti col Modello, ha la responsabilità di:

- progettare la struttura organizzativa, definendone missioni, organigrammi e funzioni.;
- definire le regole per il disegno, l'ufficializzazione e la gestione dei processi organizzativi;
- supportare la progettazione dei processi organizzativi ovvero validare procedure definite da altre funzioni, garantendone la coerenza con il disegno organizzativo complessivo;
- identificare, per ogni processo aziendale sensibile, l'Unità Organizzativa prevalente responsabile dell'autodiagnosi e dei flussi informativi destinati all'Organismo di Vigilanza;
- collaborare con le Unità Organizzative e le funzioni Compliance, Legale e Contenzioso, Internal Auditing della Capogruppo, con il Datore di lavoro, il Committente ai sensi del D. Lgs. 81/2008, il Responsabile in materia ambientale ai sensi del D. Lgs. 152/2006, ognuna per il proprio ambito di competenza, all'adeguamento del sistema normativo e del Modello (a seguito di modifiche nella normativa applicabile, nell'assetto organizzativo aziendale e/o nelle procedure operative, rilevanti ai fini del Decreto);
- diffondere la normativa interna a tutta la struttura della Società attraverso la rete Intranet aziendale.

2.6.2 Funzione Compliance della Capogruppo

Con specifico riferimento ai rischi di responsabilità amministrativa introdotti dal D. Lgs. 231/2001, la funzione Compliance della Capogruppo, anche in base a quanto previsto dal contratto di servizio in essere con Intesa Sanpaolo, supporta l'Organo di Vigilanza nello svolgimento delle sue attività di controllo mediante:

- la definizione e l'aggiornamento del Modello, in coerenza all'evoluzione della normativa di riferimento e alle modifiche della struttura organizzativa aziendale, di concerto con il Direttore Generale e con la collaborazione del Datore di lavoro, del Committente ai sensi del D. Lgs. 81/2008, del Responsabile in materia ambientale ai sensi del D. Lgs. 152/2006 e di tutte le strutture coinvolte, in base alle rispettive competenze; il monitoraggio, nel tempo, in merito alla efficacia del Modello con riferimento alle regole e principi di comportamento per la prevenzione dei reati sensibili; a tal fine la funzione Compliance:
 - individua annualmente i processi ritenuti a maggior grado di rischio in base sia a considerazioni di natura qualitativa rispetto ai reati presupposto sia all'esistenza o meno di specifici presidi a mitigazione del relativo rischio; per i processi individuati la funzione di conformità provvede al rilascio di una concordanza preventiva, anteriormente alla loro pubblicazione sul sistema normativo aziendale, circa la corretta applicazione dei principi di controllo e di comportamento previsti dal Modello; procede altresì, con un approccio *risk based*, all'effettuazione di specifiche attività di *assurance* volte a valutare la conformità dei processi ai "protocolli" previsti dal Modello;
 - analizza le risultanze del processo di autovalutazione e attestazione delle Unità Organizzative circa il rispetto dei principi di controllo e comportamento prescritti nel Modello;
- l'esame dell'informativa proveniente dalla funzione Internal Auditing della Capogruppo in merito alle criticità riscontrate nel corso della propria attività di verifica.

2.6.3 Funzione Internal Auditing della Capogruppo

Intesa Sanpaolo S.p.A. - nell'esercizio della sua peculiare funzione della Capogruppo – svolge, mediante la propria funzione Internal Auditing, periodiche verifiche volte ad assicurare in generale una costante ed indipendente azione di sorveglianza sul regolare andamento dell'operatività e dei processi al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose, valutando la funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi aziendali.

Detta funzione supporta l'Organismo di Vigilanza nel vigilare sul rispetto e sull'adeguatezza delle regole contenute nel Modello, attivando – a fronte delle eventuali criticità riscontrate nel corso della propria attività – le strutture di volta in volta competenti per le opportune azioni di mitigazione.

2.6.4 Funzione Gestione Service Segreterie Controllate della Capogruppo

La funzione Gestione Service Segreterie Controllate della Capogruppo svolge le funzioni di segreteria societaria nonché di assistenza agli Organi Societari della Società, ivi incluso l'Organismo di Vigilanza, nella risoluzione di specifiche problematiche societarie, in raccordo con le altre funzioni della Capogruppo.

2.6.5 Funzione Legale e Contenzioso della Capogruppo

La funzione Legale e Contenzioso della Capogruppo, per il perseguimento delle finalità di cui al D. Lgs. 231/2001, assicura assistenza e consulenza legale alle strutture della Società, seguendo

l'evolversi della normativa in materia di responsabilità degli enti e degli orientamenti giurisprudenziali in materia.

Spetta altresì alla funzione Legale e Contenzioso l'interpretazione della normativa, fornire riscontro a specifici quesiti legali in materia e identificare le condotte che possono configurare ipotesi di reato. La funzione Legale e Contenzioso collabora con le funzioni Compliance, Internal Auditing della Capogruppo, con il Direttore Generale, il Datore di lavoro, il Committente ai sensi del D. Lgs. 81/2008 e con il Responsabile in materia ambientale ai sensi del D. Lgs. 152/2006, all'adeguamento del Modello, segnalando anche eventuali estensioni dell'ambito di responsabilità amministrativa degli enti.

2.6.6 Funzione M&A e Partecipazioni della Capogruppo

La Funzione M&A e Partecipazioni in coerenza con il suo ruolo istituzionale, ha la responsabilità sia di assicurare consulenza e assistenza con specifico riferimento alle caratteristiche ed alle attività dell'Organismo di Vigilanza, sia di segnalare ai competenti Organi societari – in caso di operazioni societarie o di altra natura che modifichino l'ambito di operatività della Società – l'esigenza di modificare il Modello per tenere conto della nuova situazione.

2.6.7 Funzione Personale della Capogruppo

Con riferimento al D. Lgs. 231/2001, la funzione Personale della Capogruppo, come in dettaglio illustrato al Capitolo 5 e al Capitolo 6:

- programma piani di formazione e interventi di sensibilizzazione, con il supporto delle funzioni competenti e di Comunicazione Interna e Formazione, rivolti a tutto il personale (anche distaccato) sull'importanza di un comportamento conforme alle regole aziendali, sulla comprensione dei contenuti del Modello, del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo nonché specifici corsi destinati al personale che opera nelle aree sensibili con lo scopo di chiarire in dettaglio le criticità, i segnali premonitori di anomalie o irregolarità, le azioni correttive da implementare per le operazioni anomale o a rischio;
- presidia, con il supporto della funzione Internal Auditing della Capogruppo, nonché con le competenti strutture organizzative della Società, della Capogruppo - nonché delle società del Gruppo Intesa Sanpaolo di appartenenza dei dipendenti distaccati presso la Società, il processo di rilevazione e gestione delle violazioni del Modello, nonché il conseguente processo sanzionatorio e, a sua volta, fornisce tutte le informazioni emerse in relazione ai fatti e/o ai comportamenti rilevanti ai fini del rispetto della normativa del Decreto all'Organismo di Vigilanza della Società, il quale le analizza al fine di prevenire future violazioni, nonché di monitorare l'adeguatezza del Modello.

2.6.8 Datore di Lavoro e Committente ai sensi del D. Lgs. 81/2008 e Responsabile ambientale ai sensi del D. Lgs. 152/2006

I soggetti individuati quali Datore di Lavoro e Committente ai sensi del D. Lgs. 81/2008 - e/o rispettivi soggetti delegati – e Responsabile in materia ambientale ai sensi del D. Lgs. 152/2006,

limitatamente ai rispettivi ambiti di competenza per la gestione dei rischi in materia di sicurezza e salute sul lavoro e in materia ambientale:

- partecipano alla definizione della struttura del Modello e all'aggiornamento dello stesso;
- individuano e valutano l'insorgenza di fattori di rischio dai quali possano derivare la commissione di illeciti presupposto;
- promuovono le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio di non conformità.

2.6.9 Unità Organizzative della Società

Alle Unità Organizzative è assegnata la responsabilità, per quanto di propria competenza e secondo le modalità operative e le normative aziendali vigenti, dell'esecuzione, del buon funzionamento e dell'efficace applicazione nel tempo dei processi. La normativa interna individua le unità organizzative cui è assegnata la responsabilità della progettazione dei processi.

Agli specifici fini del D. Lgs. 231/2001, le Unità Organizzative hanno la responsabilità di:

- rivedere – alla luce dei principi di comportamento e di controllo prescritti per la disciplina delle attività sensibili – le prassi ed i processi di propria competenza, al fine di renderli adeguati a prevenire comportamenti illeciti;
- segnalare all'Organismo di Vigilanza eventuali situazioni di irregolarità o comportamenti anomali.

In particolare, le Unità Organizzative per le attività aziendali sensibili devono prestare la massima e costante cura nel verificare l'esistenza e nel porre rimedio ad eventuali carenze di normative o di procedure che potrebbero dar luogo a prevedibili rischi di commissione di "illeciti presupposto" nell'ambito delle attività di propria competenza.

2.7 Attività oggetto di esternalizzazione

Il modello organizzativo di AFC Digital HUB, caratterizzato da una struttura snella, prevede l'esternalizzazione (di seguito anche "*outsourcing*") di attività aziendali, o parti di esse, presso la Capogruppo e/o *outsourcer* esterni.

L'affidamento in *outsourcing* delle attività è formalizzato attraverso la stipula di specifici contratti che consentono ad AFC Digital HUB di:

- assumere ogni decisione nell'esercizio della propria autonomia, conservando le necessarie competenze e responsabilità sulle attività relative ai servizi esternalizzati;
- mantenere conseguentemente la capacità di controllo circa la congruità dei servizi resi in *outsourcing*.

I contratti di *outsourcing* prevedono apposite clausole contrattuali tra le quali:

- una descrizione dettagliata delle attività esternalizzate;
- le modalità di erogazione dei servizi;
- gli specifici livelli di servizio;
- i poteri di verifica e controllo spettanti alla Società;

- le modalità di tariffazione dei servizi resi;
- idonei sistemi di *reporting*;
- adeguati presidi a tutela del patrimonio informativo della Società;
- l'obbligo dell'*outsourcer* di operare in conformità alle leggi ed ai regolamenti vigenti nonché di esigere l'osservanza delle leggi e dei regolamenti anche da parte di terzi ai quali si dovesse rivolgere per lo svolgimento delle attività esternalizzate;
- la facoltà di AFC Digital HUB di risolvere il contratto in caso di violazione da parte dell'*outsourcer*, nella prestazione delle attività svolte in *outsourcing*: (i) delle norme legislative e delle disposizioni impartite dall'Autorità di Vigilanza che possano comportare sanzioni a carico del committente; (ii) dell'obbligo di dare esecuzione all'attività nel rispetto dei principi contenuti nel Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001 adottato da AFC Digital HUB nonché del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

Le strutture della Società verificano nel continuo, anche tramite il controllo dei previsti livelli di servizio, il rispetto delle clausole contrattuali e, di conseguenza, l'adeguatezza delle attività prestate dall'*outsourcer*.

Non sono regolate da contratti di *outsourcing* le attività svolte istituzionalmente dalla Capogruppo in tale sua qualità, tra cui quelle finalizzate a definire le linee strategiche del Gruppo e delle Società che lo compongono, volte a garantire l'uniformità nei processi e nelle azioni.

2.8 Il ruolo della Capogruppo

Ferma restando l'autonoma responsabilità di ciascuna Società appartenente al Gruppo Intesa Sanpaolo in ordine all'adozione ed all'efficace attuazione di un proprio "*Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231*", Intesa Sanpaolo, nell'esercizio della sua peculiare funzione della Capogruppo, ha il potere di impartire criteri e direttive di carattere generale e di verificare mediante le funzioni Compliance, Internal Auditing e M&A e Partecipazioni, ciascuna per quanto di rispettiva competenza, la rispondenza dei Modelli delle società appartenenti al Gruppo a tali criteri e direttive.

2.8.1 Principi di indirizzo di Gruppo in materia di Responsabilità amministrativa degli Enti

Allo scopo di uniformare a livello di Gruppo le modalità attraverso cui recepire ed attuare i contenuti del Decreto predisponendo modalità di presidio del rischio adeguate, vengono di seguito delineati i principi di indirizzo definiti dalla Capogruppo, a cui tutte le società di diritto italiano e quindi anche AFC Digital HUB, devono attenersi, nel rispetto della propria autonomia giuridica e dei principi di corretta gestione societaria.

In particolare, ciascuna società interessata deve:

- adottare il proprio Modello, dopo aver individuato le attività aziendali che presentano un rischio di commissione degli illeciti previsti dal D. Lgs. 231/2001 e le misure più idonee a prevenirne la realizzazione. Nella predisposizione del Modello la società deve attenersi ai principi e ai contenuti del Modello della Capogruppo salvo che sussistano situazioni specifiche relative alla natura,

dimensione o al tipo di attività esercitata nonché alla struttura societaria, all'organizzazione e/o all'articolazione delle deleghe interne che impongano o suggeriscano l'adozione di misure differenti al fine di perseguire più efficacemente gli obiettivi del Modello, nel rispetto comunque dei predetti principi nonché di quelli espressi nel Codice Etico, nel Codice Interno di Comportamento di Gruppo e nelle Linee Guida Anticorruzione di Gruppo. In presenza di rilevanti difformità rispetto ai principi e ai contenuti del Modello della Capogruppo devono essere trasmesse alla funzione Compliance della Capogruppo le ragioni che le hanno motivate, nonché la bozza finale del Modello prima della sua approvazione da parte degli Organi Sociali. L'avvenuta adozione del Modello è comunicata dalla Società alla predetta funzione della Capogruppo mediante trasmissione di copia del medesimo e della delibera di approvazione da parte del Consiglio di Amministrazione. Resta fermo che fino a che il Modello non sia approvato, la Società adotta ogni misura idonea per la prevenzione dei comportamenti illeciti;

- provvedere tempestivamente alla nomina dell'Organismo di Vigilanza, in linea con le indicazioni fornite dalla Capogruppo in relazione ai soggetti da nominare. L'avvenuta nomina è comunicata alle Funzioni Compliance e M&A e Partecipazioni di Intesa Sanpaolo S.p.A. Nel caso in cui i componenti dell'Organismo di Vigilanza non coincidano con quelli dell'Organo di Controllo della società controllata, dovrà essere fornita - al Comitato per il Controllo sulla Gestione della Capogruppo - specifica informativa nell'ambito della relazione sull'attività svolta dall'Organismo di Vigilanza;
- assicurare il sistematico aggiornamento del Modello in funzione di modifiche normative e organizzative, nonché nel caso in cui significative e/o ripetute violazioni delle prescrizioni del Modello lo rendessero necessario. Le modifiche normative sono segnalate alla società dalla funzione Compliance della Capogruppo con apposita comunicazione. L'avvenuto aggiornamento del Modello è comunicato alla predetta funzione Compliance con le modalità sopra illustrate;
- predisporre – coordinandosi con le Funzioni Personale e Compliance della Capogruppo – attività di formazione e di comunicazione rivolte indistintamente a tutto il Personale nonché interventi specifici di formazione destinati a figure impegnate in attività maggiormente sensibili D. Lgs. 231/2001 - tra le quali rilevano eventuali esponenti condivisi con la Capogruppo -, con l'obiettivo di creare una conoscenza diffusa e una cultura aziendale adeguata in materia;
- adottare un idoneo presidio dei processi sensibili al Decreto che preveda la loro identificazione, documentazione e pubblicazione all'interno del sistema normativo aziendale. Inoltre, tra i processi sensibili devono essere individuati annualmente dalla funzione di conformità della società o, qualora non presente, dalla funzione specificamente individuata a presidio della responsabilità amministrativa degli enti, con un approccio *risk based*, quelli ritenuti a maggior grado di rischio in base sia a considerazioni di natura qualitativa rispetto ai reati presupposto sia all'esistenza o meno di specifici presidi a mitigazione del relativo rischio. Per tali processi la Funzione di conformità provvede:
 - al rilascio di una concordanza preventiva, anteriormente alla loro pubblicazione sul sistema normativo aziendale, circa la corretta applicazione dei principi di controllo e di comportamento previsti dal Modello;

- all'effettuazione di specifiche attività di *assurance* volte a valutare la conformità dei processi ai "protocolli" previsti dal Modello;
- avviare, con cadenza annuale, il processo di autodiagnosi sulle attività svolte dalle Unità Organizzative al fine di attestare il livello di attuazione del Modello, con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative. L'attivazione del processo di autodiagnosi è effettuata coordinandosi con le Funzioni Risk Management e Compliance della Capogruppo;
- fornire alla funzione Compliance della Capogruppo copia delle relazioni periodiche, comprensive anche delle risultanze del processo di autodiagnosi, presentate dalla funzione di conformità all'Organismo di Vigilanza.

L'Organismo di Vigilanza della società provvede inoltre a trasmettere al Comitato per il Controllo sulla Gestione e all'Organismo di Vigilanza della Capogruppo, per il tramite della funzione Gestione Service Segreterie Controllate della Capogruppo, la relazione periodica, di norma semestrale, sull'attività svolta presentata dal Consiglio di Amministrazione, corredandola con le eventuali osservazioni del Consiglio stesso.

Possono essere inoltre previsti flussi informativi tra l'Organismo di Vigilanza della Capogruppo e gli Organismi delle società – anche attraverso incontri formativi su temi di comune interesse – al fine di permettere il coordinamento degli Organismi di Vigilanza del Gruppo e una migliore e più efficace vigilanza sulle misure prevenzionistiche all'interno delle singole entità societarie.

Con riferimento alle attività sopra illustrate le competenti funzioni della Capogruppo forniscono alle società supporto e collaborazione, per quanto di rispettiva competenza, nell'espletamento dei compiti alle stesse spettanti.

In ottemperanza alle Linee guida di compliance di Gruppo, per le società specificatamente individuate², la cui operatività è connotata da un elevato livello di integrazione con la Capogruppo, le attività di presidio della conformità in materia di responsabilità amministrativa degli enti sono accentrate presso la funzione Compliance della Capogruppo, fermo restando che la competenza e la responsabilità per l'approvazione e l'efficace attuazione del Modello e per la nomina dell'Organismo di Vigilanza restano in capo alle società. Sono in capo a tali società le seguenti attività:

- *iter* di formalizzazione ed approvazione del Modello presso i competenti organi sociali;
- supporto alla Capogruppo nell'acquisizione delle informazioni necessarie all'identificazione delle aree e delle attività sensibili specifiche della società;
- archiviazione e conservazione della documentazione concernente i risultati dell'autodiagnosi e delle rendicontazioni predisposte agli organi sociali;
- trasmissione alla funzione Compliance della Capogruppo di copia dell'avviso di convocazione delle riunioni dell'Organismo di Vigilanza e delle riunioni degli organi sociali qualora all'ordine del giorno rientrino argomenti connessi al D. Lgs. 231/2001.

² Sulla base di accordi/contratti di *outsourcing*.

CAPITOLO 3 L'ORGANISMO DI VIGILANZA (OdV)

3.1 Individuazione dell'Organismo di Vigilanza

Ai sensi del Decreto, il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello, nonché di curarne l'aggiornamento deve essere affidato ad un organismo interno all'Ente dotato di autonomi poteri di iniziativa e di controllo (l'"Organismo di Vigilanza").

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione e deve essere dotato di caratteristiche di autonomia, indipendenza, professionalità e continuità di azione necessarie per il corretto ed efficiente svolgimento delle funzioni ad esso assegnate; dell'avvenuta nomina dell'Organismo di Vigilanza sarà data formale comunicazione a tutti i livelli aziendali.

L'Organismo di Vigilanza è dotato di poteri di iniziativa e di controllo sulle attività della Società, senza disporre di poteri gestionali e/o amministrativi. Inoltre, onde poter svolgere, in assoluta indipendenza, le proprie funzioni, dispone di autonomi poteri di spesa sulla base di un preventivo annuale, approvato dal Consiglio di Amministrazione, previo parere positivo dell'Organismo stesso.

3.2 Composizione, durata, funzionamento e compensi dell'Organismo di Vigilanza

In considerazione dell'assetto di *governance* adottato da AFC Digital HUB, delle sue dimensioni e della complessità organizzativa e operativa della sua struttura, le funzioni di Organismo di Vigilanza sono attribuite a un organismo istituito in forma monocratica, con l'affidamento delle stesse ad un membro esterno della Società in grado di garantire autonomia, indipendenza, professionalità e onorabilità nell'esercizio dei compiti allo stesso demandati.

Il Consiglio di Amministrazione nomina il componente dell'Organismo di Vigilanza, individuandolo tra soggetti esterni in possesso dei requisiti specificati al successivo paragrafo 3.3.1.

L'Organismo di Vigilanza resta in carica per la durata stabilita dal Consiglio di Amministrazione all'atto della nomina; in assenza di una specifica determinazione, l'Organismo dura in carica per tutto il periodo in cui resta in carica il Consiglio di Amministrazione che lo ha nominato.

In caso di dimissioni, revoca, decadenza o di altra causa di cessazione del componente dell'Organismo di Vigilanza, il Consiglio di Amministrazione provvede alla nomina di un altro componente nel rispetto dei requisiti di eleggibilità previsti al paragrafo 3.3.1.

Il Consiglio di Amministrazione delibera il compenso spettante all'Organismo di Vigilanza per lo svolgimento delle relative funzioni. Al medesimo compete altresì il rimborso delle spese vive e documentate sostenute

L'Organismo di Vigilanza si avvale ordinariamente delle strutture della Società e della Capogruppo per l'espletamento dei suoi compiti di vigilanza e controllo ed *in primis* della funzione Internal Auditing della Capogruppo, istituzionalmente dotata di competenze tecniche e risorse, umane e operative, idonee a garantire lo svolgimento dei controlli, delle analisi e degli altri adempimenti necessari.

Laddove ne ravvisi la necessità, in funzione della specificità degli argomenti trattati, l'Organismo di Vigilanza può inoltre avvalersi di consulenti esterni.

Per il presidio degli ambiti normativi specialistici l'Organismo si avvale anche delle strutture interne funzionalmente competenti e dei ruoli aziendali istituiti ai sensi delle specifiche normative di settore (Datore di lavoro, Responsabile del Servizio Prevenzione e Protezione, Rappresentante dei

Lavoratori per la sicurezza, Medico competente, Responsabile ambientale ai sensi del D. Lgs. 152/2006, etc.), nonché di quelle ulteriori previste dalle normative di settore.

L'Organismo di Vigilanza, direttamente o per il tramite delle varie strutture aziendali all'uopo designate, ha accesso a tutte le attività svolte dalla Società e dagli outsourcer e alla relativa documentazione, presso le strutture della Società e degli outsourcer.

Onde poter svolgere, in assoluta indipendenza, le proprie funzioni, l'Organismo di Vigilanza dispone di autonomi poteri di spesa sulla base di un preventivo annuale, approvato dal Consiglio di Amministrazione, su proposta dell'Organismo stesso.

3.3 Requisiti di eleggibilità, cause di decadenza e sospensione

3.3.1 Requisiti di professionalità, onorabilità ed indipendenza

Il componente dell'Organismo di Vigilanza deve possedere i requisiti di professionalità, indipendenza e onorabilità di seguito specificati.

Professionalità

Il componente dell'Organismo di Vigilanza deve essere scelto tra soggetti in possesso di competenze specialistiche derivanti, ad esempio, dall'aver svolto almeno tre anni attività professionali in materie attinenti al settore nel quale la Società opera e/o dall'aver un'adeguata conoscenza dell'organizzazione, dei sistemi dei controlli e dei principali processi aziendali ovvero dell'aver fatto – o di fare – parte di Organismi di Vigilanza.

Indipendenza

Il componente dell'Organismo di Vigilanza deve possedere i requisiti di indipendenza di cui all'art. 2399 del Codice Civile.

Onorabilità

In aggiunta al possesso dei requisiti sopra richiamati, il componente dell'Organismo di Vigilanza dovrà essere in possesso dei seguenti ulteriori requisiti di onorabilità, secondo i quali non possono essere eletti componenti dell'Organismo di Vigilanza coloro i quali:

- siano stati condannati, con sentenza irrevocabile anche se a pena condizionalmente sospesa, ai sensi dell'art. 163 c.p. fatti salvi gli effetti della riabilitazione, per uno dei seguenti reati: reati per i quali è applicabile il D. Lgs. 231/2001; reati in materia di crisi d'impresa e di insolvenza³ o per i delitti fiscali. Per sentenza di condanna si intende anche quella pronunciata ai sensi dell'art. 444 c.p.p., fatti salvi gli effetti della declaratoria giudiziale di estinzione del reato ai sensi dell'art. 445, comma secondo, c.p.p.;
- abbiano rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società o enti nei cui confronti siano state applicate, con provvedimento definitivo (compresa la sentenza

³ Il riferimento è ai reati previsti dal R.D. n.267/1942 e ai reati previsti dal Codice della crisi di impresa e dell'insolvenza, (D. Lgs. n.14/2019).

emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;

- abbiano subito l'applicazione in via definitiva delle sanzioni amministrative accessorie che determinano la perdita temporanea dei requisiti di idoneità o l'interdizione temporanea allo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari o società con azioni quotate, ai sensi del D. Lgs. 58/1998 (T.U.F.) o del D. Lgs. 385/1993 (T.U.B.);
- si trovino in una delle condizioni di cui all'art. 2382 c.c.

3.3.2 Verifica dei requisiti

Il componente dell'Organismo di Vigilanza, entro trenta giorni dalla nomina, trasmette una dichiarazione al Consiglio di Amministrazione, nella quale attesta la sussistenza dei requisiti richiesti. L'infedele dichiarazione da parte del componente dell'Organismo ne determina l'immediata decadenza da tale funzione.

3.3.3 Cause di decadenza

Il componente dell'Organismo di Vigilanza, successivamente alla sua nomina, decade da tale carica, qualora venga meno uno dei requisiti di professionalità, di indipendenza o di onorabilità stabiliti come condizione per l'eleggibilità, ai sensi del precedente paragrafo 3.3.1;

L'Organismo di Vigilanza deve comunicare al Presidente del Consiglio di Amministrazione, sotto la sua piena responsabilità, il sopravvenire di una delle cause di decadenza.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una causa di decadenza, convoca senza indugio il Consiglio di Amministrazione affinché proceda – nella sua prima riunione successiva all'avvenuta conoscenza – alla dichiarazione di decadenza dell'Organismo di Vigilanza e alla nomina di un nuovo Organismo.

3.3.4 Cause di sospensione, temporaneo impedimento e revoca

Costituiscono cause di sospensione dalla funzione di componente dell'Organismo di Vigilanza:

- i casi in cui il Consiglio di Amministrazione accerti, dopo la nomina, che il componente dell'Organismo ha rivestito il medesimo ruolo in una società o ente nei cui confronti siano state applicate, con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti dell'ente commessi durante la sua carica;
- la sentenza di condanna non definitiva, alla quale è equiparata la sentenza emessa ai sensi dell'art. 444 c.p.p., anche a pena sospesa, per uno dei seguenti reati: reati per i quali è applicabile il D. Lgs. 231/2001; reati in materia di crisi d'impresa e di insolvenza o per i delitti fiscali;
- il rinvio a giudizio per uno dei reati previsti al punto che precede;
- l'applicazione in via non definitiva delle sanzioni amministrative accessorie che determinano la perdita temporanea dei requisiti di idoneità o l'interdizione temporanea allo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari o società con azioni quotate, ai sensi del D. Lgs. 58/1998 (T.U.F.) o del D. Lgs. 385/1993 (T.U.B.).

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, al componente dell'Organismo di Vigilanza di svolgere le proprie funzioni ovvero di svolgerle con la necessaria indipendenza e autonomia di giudizio, questi è tenuto a dichiarare la sussistenza del legittimo impedimento al Consiglio di Amministrazione, e, qualora esso sia dovuto ad un potenziale conflitto di interessi, la causa da cui il medesimo deriva.

Costituiscono inoltre cause di temporaneo impedimento la malattia o l'infortunio o altro giustificato impedimento che si protragga per oltre tre mesi e impediscano all'Organismo di Vigilanza di assolvere ai propri compiti.

L'Organismo di Vigilanza deve comunicare al Presidente del Consiglio di Amministrazione, sotto la sua piena responsabilità, il sopravvenire di una delle cause di sospensione o di temporaneo impedimento di cui sopra.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una delle cause di sospensione o temporaneo impedimento citate, ne informa senza indugio il Consiglio di Amministrazione affinché proceda – nella sua prima riunione successiva all'avvenuta conoscenza – a dichiarare la sospensione della carica o a prendere atto del temporaneo impedimento.

Nell'ipotesi di sospensione o di temporaneo impedimento del componente dell'Organismo, il Consiglio di Amministrazione dispone la nomina pro-tempore di un componente "supplente", comunque in possesso dei requisiti di professionalità, indipendenza e onorabilità specificati al precedente paragrafo 3.3.1.

La sospensione non può durare oltre sei mesi, trascorsi i quali il Presidente del Consiglio di Amministrazione iscrive l'eventuale revoca del componente sospeso fra le materie da trattare nella prima riunione del Consiglio successiva a tale termine. Il componente non revocato è reintegrato nel pieno delle funzioni.

In caso di temporaneo impedimento che si protragga per un periodo superiore a sei mesi, il Consiglio di Amministrazione ha facoltà di addivenire alla eventuale revoca dell'Organismo di Vigilanza e alla sua sostituzione.

Il Consiglio di Amministrazione può revocare (e nominare un nuovo Organismo di Vigilanza), con delibera motivata, in ogni tempo il componente dell'Organismo di Vigilanza qualora accerti che si sia reso responsabile di un grave inadempimento nell'assolvimento dei compiti oggetto dell'incarico, previo parere conforme del Sindaco Unico.

3.4 Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza, nell'esecuzione della sua attività ordinaria, vigila:

- sull'efficienza, efficacia ed adeguatezza del Modello e delle disposizioni dallo stesso richiamate nel prevenire e contrastare la commissione degli illeciti per i quali è applicabile il D. Lgs. 231/2001, anche di quelli che in futuro dovessero comunque comportare una responsabilità amministrativa della persona giuridica;

- sull'osservanza delle prescrizioni contenute nel Modello e delle disposizioni dallo stesso richiamate da parte dei destinatari, rilevando la coerenza e gli eventuali scostamenti dei comportamenti attuati, attraverso l'analisi dei flussi informativi e le segnalazioni alle quali sono tenuti i responsabili delle varie Unità Organizzative;
- sull'aggiornamento del Modello non appena si riscontrino esigenze di adeguamento, formulando proposte agli Organi Societari competenti, laddove si rendano opportune modifiche e/o integrazioni in conseguenza di significative violazioni delle prescrizioni del Modello stesso, di significativi mutamenti dell'assetto organizzativo e procedurale della Società, nonché delle novità legislative intervenute in materia;
- sull'esistenza ed effettività del sistema aziendale di prevenzione e protezione in materia di salute e sicurezza sui luoghi di lavoro;
- sull'attuazione delle attività formative del Personale, di cui al successivo paragrafo 6.2;
- sull'adeguatezza delle procedure e dei canali per la segnalazione interna di condotte illecite rilevanti ai fini del D. Lgs. 231/2001 o di violazioni del Modello e sulla loro idoneità a garantire la riservatezza dell'identità del segnalante nelle attività di gestione delle segnalazioni;
- sul rispetto del divieto di porre in essere "atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione";
- sull'avvio e sullo svolgimento del procedimento di irrogazione di un'eventuale sanzione disciplinare, a seguito dell'accertata violazione del Modello;
- sul rispetto dei principi e dei valori contenuti nel Codice Etico.

L'Organismo di Vigilanza, nel perseguimento della finalità di vigilare sull'effettiva attuazione del Modello, svolge attività di controllo sulla base di un "Piano delle verifiche 231" elaborato con il supporto delle funzioni Compliance e Internal Auditing della Capogruppo, tenendo conto del grado di rischio delle attività sensibili della Società.

Tale Piano, predisposto annualmente, tiene anche conto delle eventuali osservazioni e indicazioni ricevute a vario titolo da parte degli Organi Societari.

Durante gli interventi di controllo viene analizzato nel dettaglio il livello di controlli presenti nell'operatività e nei processi aziendali. I punti di debolezza rilevati sono sistematicamente segnalati alle Unità Organizzative interessate al fine di rendere più efficienti ed efficaci le regole, le procedure e la struttura organizzativa. Al fine di verificare l'effettiva attuazione delle azioni di mitigazione da intraprendere sui contesti di rischio segnalati, viene svolta un'attività di sorveglianza sull'avanzamento degli interventi, nonché dei riscontri di *follow-up* (ove necessario).

Le competenti Unità Organizzative che eventualmente supportano l'Organismo nell'ambito di tali attività rendicontano periodicamente all'Organismo stesso.

L'Organismo di Vigilanza può scambiare informazioni con il Sindaco Unico e la Società di Revisione, se ritenuto necessario o opportuno nell'ambito dell'espletamento delle rispettive competenze e responsabilità e, sempre ove ritenuto opportuno, può chiedere al Presidente del Consiglio di Amministrazione e agli altri Consiglieri, nell'ambito delle materie di competenza del Consiglio medesimo, specifiche informazioni su temi che ritiene necessario approfondire per svolgere al meglio i propri compiti di vigilanza sul funzionamento, efficacia e osservanza del Modello.

3.5 Modalità e periodicità di riporto agli Organi Societari

L'Organismo di Vigilanza in ogni circostanza in cui sia ritenuto necessario o opportuno, ovvero se richiesto, riferisce al Consiglio di Amministrazione circa il funzionamento del Modello e l'adempimento agli obblighi imposti dal Decreto.

L'Organismo di Vigilanza, su base almeno semestrale, trasmette al Consiglio di Amministrazione una specifica informativa sull'adeguatezza e sull'osservanza del Modello, che ha ad oggetto:

- l'attività svolta;
- le risultanze dell'attività svolta;
- gli interventi correttivi e migliorativi pianificati ed il loro stato di realizzazione.

A seguito dell'esame da parte del Consiglio di Amministrazione, l'Organismo di Vigilanza provvede ad inoltrare l'informativa – comprensiva delle osservazioni eventualmente formulate dal Consiglio di Amministrazione – al Comitato per il Controllo sulla Gestione e all'Organismo di Vigilanza della Capogruppo, per il tramite della funzione Gestione Service Segreterie Controllate della Capogruppo.

CAPITOLO 4 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

4.1 Flussi informativi da effettuarsi al verificarsi di particolari eventi ed in caso di segnalazioni *whistleblowing*

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte del Personale, dei Responsabili delle strutture e Funzioni Aziendali, degli Organi Societari, dei soggetti esterni (intendendosi per tali i fornitori, gli agenti, i consulenti, i professionisti, i lavoratori autonomi o parasubordinati, i professionisti, i fornitori, i *partner* commerciali, o altri soggetti) in merito ad eventi che potrebbero ingenerare responsabilità di AFC Digital HUB ai sensi del Decreto.

Devono essere senza ritardo segnalate le notizie circostanziate, fondate su elementi di fatto precisi e concordanti, concernenti:

- la commissione, o la ragionevole convinzione di commissione, degli illeciti per i quali è applicabile il D. Lgs. 231/2001;
- le violazioni delle regole di comportamento o procedurali contenute nel presente Modello e nella normativa interna in esso richiamata;
- l'avvio di procedimenti giudiziari a carico dei destinatari del Modello per reati previsti nel D. Lgs. 231/2001.

Le segnalazioni possono essere effettuate, anche in forma anonima:

- direttamente all'Organismo di Vigilanza, tramite:
 - lettera all'indirizzo "Anti Financial Crime Digital Hub S.c.a.r.l. - Organismo di Vigilanza - c/o Intesa Sanpaolo S.p.A. - Gestione Service Segreterie Controllate - Via Romagnosi 5 - 20121 Milano"ovvero
 - e-mail alla casella di posta elettronica OrganismoDiVigilanzaDL231@afcdigitalhub.com;
- per il tramite della funzione Internal Auditing della Capogruppo, alla quale la segnalazione potrà essere effettuata tanto direttamente quanto mediante il Responsabile della struttura di appartenenza; la funzione Internal Auditing della Capogruppo, esperiti i debiti approfondimenti, informa l'Organismo di Vigilanza in merito alle segnalazioni pervenute e lo rendiconta sui fatti al riguardo riscontrati.

I soggetti esterni, ivi compresi i soggetti che svolgono attività in *outsourcing* per conto della Società, possono inoltrare la segnalazione direttamente all'Organismo di Vigilanza con una delle modalità sopra indicate.

Inoltre, ai sensi delle varie fonti normative che prevedono l'adozione di sistemi interni di segnalazione delle violazioni delle disposizioni che regolamentano specifici settori (T.U.B., T.U.F., normativa antiriciclaggio, ecc.), le segnalazioni possono essere effettuate dal personale⁴, necessariamente in forma non anonima, secondo le disposizioni dettate dalle "Regole di Gruppo sui sistemi interni di

⁴ Ai sensi delle Regole di Gruppo sui sistemi interni di segnalazione delle violazioni (*whistleblowing*) per "personale" deve intendersi: "i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato".

segnalazione delle violazioni (*whistleblowing*)⁵ tramite l'invio di una mail all'indirizzo segnalazioni.violazioni@intesanpaolo.com a cui ha accesso il Chief Audit Officer (in veste di "Responsabile dei sistemi interni di segnalazione") ed il suo Delegato.

Qualora a causa della natura della segnalazione la struttura Chief Audit Officer possa potenzialmente trovarsi in una situazione di conflitto di interesse, è inoltre previsto un canale di "riserva" alternativo che fa capo al Comitato per il Controllo sulla Gestione:

segnalazioniviolazioni.comitatoperilcontrollo@intesanpaolo.com.

Le segnalazioni così pervenute, dopo un primo esame di merito, vengono quindi subito inviate alla funzione competente – individuata in base alla fattispecie evidenziata – ai fini dell'avvio dei necessari accertamenti.

La funzione incaricata, come previsto nelle "Regole di Gruppo sui sistemi interni di segnalazione delle violazioni (*whistleblowing*)", deve fornire tempestiva informativa all'Organismo di Vigilanza (OdV), in presenza di tematiche sensibili ai fini del D. Lgs. 231/2001.

L'Organismo di Vigilanza valuta le segnalazioni ricevute direttamente e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna.

L'Organismo di Vigilanza prenderà in considerazione le segnalazioni, ancorché anonime, che presentino elementi fattuali.

La Società garantisce, qualunque sia il canale utilizzato, i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione e assicura in ogni caso la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge. Ai sensi dell'art.6 del Decreto:

- sono vietati atti di ritorsione o discriminatori, diretti o indiretti nei confronti del segnalante, per motivi collegati, direttamente o indirettamente, alla segnalazione. Sono nulli il licenziamento ritorsivo e le misure organizzative aventi effetti negativi diretti o indiretti sulle condizioni di lavoro, se non sia dimostrato che non abbiano natura ritorsiva e che si fondino su ragioni estranee alla segnalazione;
- l'adozione di misure discriminatorie può essere denunciata all'Ispettorato nazionale del lavoro;
- il sistema disciplinare previsto dal Decreto, in attuazione del quale sono stabilite le sanzioni indicate nel Capitolo 5 che segue, si applica anche a chi:
 - viola gli obblighi di riservatezza sull'identità del segnalante o i divieti di atti discriminatori o ritorsivi;
 - effettua con dolo o colpa grave segnalazioni di fatti che risultino infondati.

Oltre alle segnalazioni relative alle violazioni sopra descritte, devono obbligatoriamente ed immediatamente essere trasmesse all'Organismo:

- per il tramite della funzione Internal Auditing o della funzione Legale della Capogruppo, le informazioni concernenti i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali

⁵ In corso di recepimento.

si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti per i quali è applicabile il D. Lgs. 231/2001, qualora tali indagini coinvolgano la Società o il Personale od Organi Societari o comunque la responsabilità di AFC Digital HUB stessa;

- per il tramite della funzione Internal Auditing della Capogruppo, l'informativa su fatti, atti, eventi e omissioni con profili di grave criticità rispetto all'osservanza delle norme del Decreto, rilevati dalle funzioni di controllo aziendali nell'ambito delle loro attività e le relative azioni correttive.

Ciascuna Unità Organizzativa a cui sia attribuito un determinato ruolo in una fase di un processo sensibile deve segnalare tempestivamente all'Organismo di Vigilanza eventuali propri comportamenti significativamente difformi da quelli descritti nel processo e le motivazioni che hanno reso necessario od opportuno tale scostamento.

La funzione Internal Auditing della Capogruppo, in caso di eventi che potrebbero ingenerare responsabilità della Società ai sensi del D. Lgs. 231/2001, informa tempestivamente l'Organismo di Vigilanza e predisponde specifica relazione che descriva nel dettaglio l'evento stesso, il rischio, il personale coinvolto, i provvedimenti disciplinari in corso e le soluzioni per limitare il ripetersi dell'evento.

4.2 Flussi informativi periodici

L'Organismo di Vigilanza esercita le proprie responsabilità di controllo anche mediante l'analisi di sistematici flussi informativi periodici trasmessi dalle Unità Organizzative che svolgono attività di controllo di primo livello, dalle funzioni Compliance e Internal Auditing della Capogruppo, nonché, per quanto concerne gli ambiti normativi specialistici, dalle altre strutture interne e della Capogruppo funzionalmente competenti e dai ruoli aziendali istituiti ai sensi delle specifiche normative di settore (ad es. Datore di Lavoro e Committente ai sensi del D. Lgs. 81/2008).

4.2.1 Flussi informativi provenienti dalle Unità Organizzative

Con cadenza annuale, i responsabili delle Unità Organizzative aziendali coinvolte nei processi "sensibili" ai sensi del D. Lgs. 231/2001, mediante un processo di autodiagnosi complessivo sull'attività svolta, attestano il livello di attuazione del Modello con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative.

Attraverso questa formale attività di autovalutazione, evidenziano le eventuali criticità nei processi gestiti, gli eventuali scostamenti rispetto alle indicazioni dettate dal Modello o più in generale dall'impianto normativo, l'adeguatezza della medesima regolamentazione, con l'evidenziazione delle azioni e delle iniziative adottate o al piano per la soluzione.

Le attestazioni delle Unità sono inviate con cadenza annuale alla Funzione Compliance della Capogruppo, la quale archiverà la documentazione, tenendola a disposizione dell'Organismo di Vigilanza, per il quale produrrà una relazione con le risultanze.

4.2.2 Flussi informativi da parte dalla Funzione Compliance della Capogruppo

I flussi di rendicontazione della Funzione Compliance della Capogruppo consistono nella predisposizione e presentazione di relazioni annuali all'Organismo di Vigilanza, con le quali viene

comunicato l'esito dell'attività svolta in relazione all'adeguatezza, osservanza ed al funzionamento del Modello, alle variazioni intervenute nei processi e nelle procedure (avvalendosi, a tal fine della collaborazione del Direttore Generale) nonché agli interventi correttivi e migliorativi pianificati (inclusi quelli formativi) ed al loro stato di realizzazione.

Per il documento citato è previsto un aggiornamento semestrale.

4.2.3 Flussi informativi da parte della funzione Internal Auditing della Capogruppo

Il flusso di rendicontazione della funzione Internal Auditing della Capogruppo verso l'Organismo di Vigilanza è incentrato su relazioni annuali, con le quali quest'ultimo è informato sulle verifiche svolte che abbiano avuto per oggetto la Società e sugli ulteriori interventi di controllo in programma nell'esercizio successivo.

Nell'ambito di tale rendicontazione è data evidenza di sintesi delle segnalazioni i cui approfondimenti hanno evidenziato tematiche sensibili ai fini del D. Lgs. 231/2001.

Laddove ne ravvisi la necessità, l'Organismo di Vigilanza richiede alla funzione Internal Auditing della Capogruppo copia dei report di dettaglio per i punti specifici che ritiene di voler meglio approfondire.

Inoltre, a fronte dell'eventuale svolgimento, d'iniziativa o su richiesta dell'Organismo di Vigilanza, di specifiche verifiche attinenti ad aree sensibili ai fini del D. Lgs. 231/2001, la funzione Internal Auditing della Capogruppo invierà all'Organismo stesso copia dei *report* di dettaglio.

4.2.4 Flussi informativi da parte del Datore di lavoro ai sensi del D. Lgs. 81/2008

Il flusso di rendicontazione del Datore di lavoro ai sensi del D. Lgs. 81/2008 verso l'Organismo di Vigilanza è incentrato su relazioni con cadenza almeno annuale con le quali viene comunicato l'esito della attività svolta in relazione alla organizzazione ed al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza.

4.2.5 Flussi informativi da parte del Committente ai sensi del D. Lgs. 81/2008

Il flusso di rendicontazione del Committente ai sensi degli artt. 88 e segg. del D. Lgs. 81/2008 verso l'Organismo di Vigilanza è incentrato su relazioni con cadenza almeno annuale con le quali viene comunicato l'esito della attività svolta in relazione alla organizzazione ed al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza nei cantieri temporanei o mobili.

4.2.6 Flussi informativi da parte del Responsabile Ambientale

Il flusso di rendicontazione del Responsabile in materia ambientale ai sensi del D. Lgs. 152/2006 verso l'Organismo di Vigilanza è incentrato su relazioni con cadenza almeno annuale sul rispetto delle disposizioni previste dalla normativa ambientale e il presidio dell'evoluzione normativa nonché l'esito della attività svolta in relazione alla organizzazione ed al controllo effettuato sul sistema di gestione ambientale.

4.2.7 Flussi informativi da parte della Funzione Personale della Capogruppo

Il flusso di rendicontazione prodotto dalla Funzione Personale della Capogruppo consiste in una informativa con cadenza almeno annuale concernente i provvedimenti disciplinari comminati al personale dipendente nel periodo di riferimento, con particolare evidenza degli eventi collegati direttamente o indirettamente a segnalazioni di condotte illecite previste dal Decreto ovvero violazioni del Modello. Laddove i provvedimenti riguardino fatti, atti, eventi e omissioni con profili di grave criticità rispetto all'osservanza delle norme del Decreto vi potrà essere un'informativa specifica al di fuori dell'ordinaria rendicontazione.

4.2.8 Flussi informativi da parte del Direttore Generale

Il flusso di rendicontazione consiste in una informativa con periodicità annuale concernente le principali variazioni intervenute nella struttura organizzativa, la loro rilevanza ex D. Lgs. 231/2001, nonché lo stato di allineamento del sistema dei poteri (facoltà, deleghe e poteri).

CAPITOLO 5 IL SISTEMA SANZIONATORIO

5.1 Il sistema sanzionatorio

5.1.1 Principi generali

L'efficacia del Modello è assicurata – oltre che dall'elaborazione di meccanismi di decisione e di controllo tali da eliminare o ridurre significativamente il rischio di commissione degli illeciti penali ed amministrativi per i quali è applicabile il D. Lgs. 231/2001 – dagli strumenti sanzionatori posti a presidio dell'osservanza delle condotte prescritte.

I comportamenti del Personale di AFC Digital HUB e dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i *partner*, ecc.) non conformi ai principi e alle regole di condotta prescritti nel presente Modello – ivi ricomprendendo il Codice Etico, il Codice Interno di Comportamento di Gruppo, le Linee Guida Anticorruzione di Gruppo e le procedure e norme interne, che fanno parte integrante del Modello – costituiscono illecito contrattuale.

Su tale presupposto, la Società adoterà nei confronti:

- dei membri degli Organi Sociali della Società, l'eventuale segnalazione agli Organi stessi affinché assumano eventuali iniziative amministrative nei loro riguardi;
- dell'eventuale personale dipendente assunto presso AFC Digital HUB con contratto regolato dal diritto italiano e dai contratti collettivi nazionali di settore, il sistema sanzionatorio stabilito dal Codice disciplinare della Società e dalle leggi e norme contrattuali di riferimento;
- dei dipendenti della Capogruppo e/o di altre società del Gruppo che, in regime di distacco, prestano la propria attività professionale presso AFC Digital HUB (cosiddetti dipendenti distaccati da altre società del Gruppo), le misure opportune affinché le competenti strutture delle società di appartenenza applichino il sistema sanzionatorio stabilito dal Codice disciplinare delle società di appartenenza medesime e dalle leggi e norme contrattuali di riferimento;
- di tutti i soggetti esterni, il sistema sanzionatorio stabilito dalle disposizioni contrattuali e di legge che regolano la materia.

Qualora la Società assumesse direttamente personale, l'attivazione, sulla base delle segnalazioni pervenute dalle competenti strutture della Società, della Capogruppo o dall'Organismo di Vigilanza, lo svolgimento e la definizione del procedimento disciplinare nei confronti dell'eventuale Personale dipendente saranno affidati, nell'ambito delle competenze alla stessa attribuite, alla Funzione Personale della Capogruppo, in coordinamento con il Direttore Generale.

Gli interventi sanzionatori nei confronti dei soggetti esterni sono affidati alla funzione competente su indicazione di eventuali fatti rilevanti da parte della struttura interna ovvero della competente struttura della Capogruppo/altre società del Gruppo che gestisce il contratto o presso cui opera il lavoratore autonomo ovvero il fornitore, le quali possono prestare il loro supporto alla funzione competente.

Il tipo e l'entità di ciascuna delle sanzioni stabilite, saranno applicate, ai sensi della normativa richiamata, tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione, tenuto altresì conto di eventuale recidiva, nonché

dell'attività lavorativa svolta dall'interessato e della relativa posizione funzionale, unitamente a tutte le altre particolari circostanze che possono aver caratterizzato il fatto.

Quanto precede verrà adottato indipendentemente dall'avvio e/o svolgimento e definizione dell'eventuale azione penale, in quanto i principi e le regole di condotta imposte dal Modello sono assunte dalla Società in piena autonomia ed indipendentemente dai possibili reati che eventuali condotte possano determinare e che l'Autorità Giudiziaria ha il compito di accertare.

La verifica dell'adeguatezza del sistema sanzionatorio, il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti del Personale, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'Organismo di Vigilanza, il quale riceve dalla funzione Personale un'informativa con cadenza annuale sui provvedimenti disciplinari comminati al personale dipendente nel periodo di riferimento.

In applicazione dei suddetti criteri, è di seguito riportato il sistema sanzionatorio applicabile.

5.1.2 Personale dipendente eventualmente assunto da AFC Digital HUB appartenente alle aree professionali e ai quadri direttivi

Si riporta di seguito il sistema sanzionatorio previsto per i dipendenti (aree professionali e quadri direttivi) con contratto di lavoro regolato dal diritto italiano.

1) il provvedimento del rimprovero verbale si applica in caso:

di lieve inosservanza dei principi e delle regole di comportamento previsti dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello, correlandosi detto comportamento ad una *“lieve inosservanza delle norme contrattuali, o delle direttive ed istruzioni delle regole aziendali o delle direttive o istruzioni impartite dalla direzione o dai superiori”* ai sensi di quanto già previsto al punto a) del Codice disciplinare vigente;

2) il provvedimento del rimprovero scritto si applica in caso:

di inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da poter essere considerata ancorché non lieve, comunque, non grave, correlandosi detto comportamento ad una *“inosservanza non grave delle norme contrattuali, o delle direttive ed istruzioni delle regole aziendali o delle direttive o istruzioni impartite dalla direzione o dai superiori”* ai sensi di quanto previsto al punto b) del Codice disciplinare vigente;

3) il provvedimento della sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni si applica in caso:

di inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni

del Modello in misura tale da essere considerata di una certa gravità, anche se dipendente da recidiva, correlandosi detto comportamento ad una *“inosservanza - ripetuta o di una certa gravità - delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori”* ai sensi di quanto previsto al punto c) del Codice disciplinare vigente;

4) il provvedimento del licenziamento per giustificato motivo si applica in caso: di adozione, nell’espletamento delle attività ricomprese nelle aree sensibili, di un comportamento caratterizzato da notevole inadempimento delle prescrizioni e/o delle procedure e/o delle norme interne stabilite dal presente Modello, anche se sia solo suscettibile di configurare uno degli illeciti per i quali è applicabile il Decreto, correlandosi detto comportamento ad una *“violazione (. . .) tale da configurare (. . .) un inadempimento “notevole” degli obblighi relativi”* ai sensi di quanto previsto al punto d) del Codice disciplinare vigente;

5) il provvedimento del licenziamento per giusta causa si applica in caso: di adozione, nell’espletamento delle attività ricomprese nelle aree sensibili, di un comportamento consapevole in contrasto con le prescrizioni e/o le procedure e/o le norme interne del presente Modello, che, ancorché sia solo suscettibile di configurare uno degli illeciti per i quali è applicabile il Decreto, leda l’elemento fiduciario che caratterizza il rapporto di lavoro ovvero risulti talmente grave da non consentirne la prosecuzione, neanche provvisoria, correlandosi detto comportamento ad una *“mancanza di gravità tale (o per la doloosità del fatto, o per i riflessi penali o pecuniari o per la recidività, o per la sua particolare natura) da far venir meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentire comunque la prosecuzione nemmeno provvisoria del rapporto stesso”* ai sensi di quanto previsto alla lettera e) del Codice disciplinare vigente.

5.1.3 Personale dirigente

In caso di violazione, da parte di dirigenti, dei principi, delle regole e delle procedure interne previste dal Modello o di adozione, nell’espletamento di attività ricomprese nelle aree sensibili di un comportamento non conforme alle prescrizioni del Modello stesso, il Consiglio di Amministrazione adotterà le necessarie deliberazioni, tenendo conto della gravità della/e violazione/i, della eventuale reiterazione e del venir meno del rapporto fiduciario cui si ispira il rapporto di collaborazione professionale tra la Società e il lavoratore con la qualifica di dirigente, sempre in conformità con quanto previsto dalle vigenti disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro, si procederà con il licenziamento con preavviso e il licenziamento per giusta causa che, comunque, andranno applicati nei casi di massima gravità della violazione commessa.

Considerato che detti provvedimenti comportano la risoluzione del rapporto di lavoro, la Società, in attuazione del principio legale della gradualità della sanzione, si riserva la facoltà, per le infrazioni, meno gravi, di applicare la misura del rimprovero scritto – in caso di semplice inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell’ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello – ovvero la misura della sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni

in caso di inadempimento colposo di una certa rilevanza (anche se dipendente da recidiva) ovvero di condotta colposa inadempiente ai principi e alle regole di comportamento previsti dal Modello.

5.1.4 Personale dipendente distaccato dalla Capogruppo e/o da altre società del Gruppo

I dipendenti della Capogruppo e/o di altre società del Gruppo che, in regime di distacco, prestano la propria attività professionale presso la Società saranno assoggettati al sistema sanzionatorio / disciplinare previsto nei rispettivi Modelli adottati dalle suddette società.

Le funzioni competenti della società di appartenenza provvederanno, sulla base delle segnalazioni pervenute anche dall'Organismo di Vigilanza della Società, all'applicazione del sistema sanzionatorio disciplinato all'interno del proprio Modello, dandone informativa al Consiglio di Amministrazione di AFC Digital HUB.

5.1.5 Soggetti esterni

Ogni comportamento posto in essere da soggetti esterni alla Società che, in contrasto con il Modello, sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i quali è applicabile il Decreto, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di convenzione, la risoluzione anticipata del rapporto contrattuale, fatta ovviamente salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti alla Società, come nel caso di applicazione da parte dell'Autorità Giudiziaria delle sanzioni previste dal Decreto.

5.1.6 Componenti del Consiglio di Amministrazione e Sindaco Unico

In caso di violazione del Modello da parte di soggetti che ricoprono la funzione di componenti del Consiglio di Amministrazione o di Sindaco Unico della Società, l'Organismo di Vigilanza, avuta notizia della violazione, provvederà ad informare il Consiglio di Amministrazione e il Sindaco Unico nel primo caso e il solo Consiglio di Amministrazione nel secondo caso, al fine di consentire agli stessi l'adozione delle iniziative ritenute opportune in relazione alla fattispecie, nel rispetto della normativa vigente.

CAPITOLO 6 COMUNICAZIONE INTERNA E FORMAZIONE

Il regime della responsabilità amministrativa previsto dalla normativa di legge e l'adozione del Modello di organizzazione, gestione e controllo da parte della Società formano un sistema che deve trovare nei comportamenti operativi del Personale una coerente ed efficace risposta.

Al riguardo è fondamentale un'attività di comunicazione e di formazione finalizzata a favorire la diffusione di quanto stabilito dal Decreto e dal Modello adottato nelle sue diverse componenti (gli strumenti aziendali presupposto del Modello, le finalità del medesimo, la sua struttura e i suoi elementi fondamentali, il sistema dei poteri e delle deleghe, l'individuazione dell'Organismo di Vigilanza, i flussi informativi verso quest'ultimo, le tutele previste per chi segnala fatti illeciti, etc.). Ciò affinché la conoscenza della materia e il rispetto delle regole che dalla stessa discendono costituiscano parte integrante della cultura degli esponenti aziendali e di ciascun collaboratore.

Con questa consapevolezza, le attività di formazione e comunicazione interna – rivolte e a tutto il Personale – hanno il costante obiettivo, anche in funzione degli specifici ruoli assegnati, di creare una conoscenza diffusa e una cultura aziendale adeguata alle tematiche in questione, mitigando così il rischio della commissione di illeciti.

6.1 Comunicazione interna

Gli eventuali neoassunti da AFC Digital HUB ricevono, all'atto della assunzione, unitamente alla prevista restante documentazione, copia del Modello della Società, del Codice Etico e del Codice Interno di Comportamento e delle Linee Guida Anticorruzione del Gruppo.

La sottoscrizione di un'apposita dichiarazione attesta la consegna dei documenti, l'integrale conoscenza dei medesimi e l'impegno ad osservare le relative prescrizioni.

I dipendenti distaccati dalla Capogruppo e/o da altre società del Gruppo che prestano la propria attività lavorativa presso AFC Digital HUB prendono visione, all'atto del distacco, del Modello della Società.

Sull'intranet aziendale, sono pubblicati e resi disponibili per la consultazione, oltre alle varie comunicazioni interne, il Modello e le normative collegate (in particolare, Codice Etico, Codice Interno di Comportamento e Linee Guida Anticorruzione di Gruppo).

I documenti pubblicati sono costantemente aggiornati in relazione alle modifiche che via via intervengono nell'ambito della normativa di legge e del Modello, i cui periodici aggiornamenti sono comunicati dal vertice aziendale a tutto il Personale.

L'attività di comunicazione interna a supporto del Decreto e del Modello, si avvale di una pluralità di strumenti.

Il sito Notizie Interne di Intranet e la *Web Tv* di Intesa Sanpaolo S.p.A, quest'ultima nelle modalità *Live* e *On Demand*, sono gli strumenti in grado di informare in tempo reale il Personale delle novità intervenute; la *Web Tv*, in particolare, con apposite trasmissioni (*clip*), contenenti anche interviste ai vari Responsabili, è uno strumento in grado di proporre adeguati momenti di approfondimento sulla normativa in materia, sulle attività "sensibili", sugli interventi formativi, ecc.

L'*house organ* di Intesa Sanpaolo S.p.A. e la pubblicazione di materiale di comunicazione di tipo divulgativo (ad es. *vademecum*/quaderni monografici) sono gli strumenti destinati ad ospitare

periodici articoli di approfondimento redatti anche con il contributo di esperti, nonché contributi sul Decreto il cui obiettivo è quello di favorire la diffusione ed il consolidamento della conoscenza in tema di responsabilità amministrativa degli enti.

In sintesi, l'insieme degli strumenti citati, unitamente alle circolari interne, garantisce a tutto il Personale una informazione completa e tempestiva.

6.2 Formazione

Le iniziative formative hanno l'obiettivo di far conoscere il Decreto, il Modello e, in particolare, di sostenere adeguatamente gli esponenti aziendali, il personale e coloro che sono coinvolti nelle attività "sensibili".

Per garantirne l'efficacia esse sono erogate tenendo conto delle molteplici variabili presenti nel contesto di riferimento; in particolare:

- i *target* (i destinatari degli interventi, il loro livello e ruolo organizzativo);
- i contenuti (gli argomenti attinenti al ruolo delle persone);
- gli strumenti di erogazione (formazioni *live*, *digital*);
- i tempi di erogazione e di realizzazione (la preparazione e la durata degli interventi);
- l'impegno richiesto al *target* (i tempi di fruizione);
- le azioni necessarie per il corretto sostegno dell'intervento (promozione, supporto dei Capi).

Le attività prevedono:

- una formazione digitale destinata a tutto il personale;
- specifiche iniziative formative per gli esponenti aziendali e per le persone che lavorano nelle strutture in cui maggiore è il rischio di comportamenti illeciti;
- altri strumenti formativi di approfondimento da impiegare attraverso la piattaforma della formazione.

La piattaforma consente a ciascun partecipante di consultare i contenuti formativi di base sul Decreto, oltre ad eventuali aggiornamenti legislativi, e verificare il proprio livello di apprendimento attraverso un test finale.

La formazione specifica interviene laddove necessario, a completamento della fruizione dei contenuti digitali destinati a tutto il personale e ha l'obiettivo di diffondere la conoscenza dei reati, delle fattispecie configurabili, dei presidi specifici relativi alle aree di competenza degli operatori, e di richiamare alla corretta applicazione del Modello di organizzazione, gestione e controllo. La metodologia didattica è fortemente interattiva e si avvale di case studies.

I contenuti formativi digitali e gli interventi specifici sono aggiornati in relazione all'evoluzione della normativa esterna e del Modello. Se intervengono modifiche rilevanti (ad esempio, estensione della responsabilità amministrativa dell'ente a nuove tipologie di reati), si procede ad una coerente integrazione dei contenuti medesimi, assicurandone altresì la fruizione.

La fruizione delle varie iniziative di formazione è obbligatoria per gli esponenti aziendali e per tutto il Personale cui le iniziative stesse sono dirette ed è monitorata a cura della funzione Personale della

Capogruppo, con la collaborazione dei responsabili ai vari livelli che devono farsi garanti, in particolare, della fruizione delle iniziative di formazione “a distanza” da parte dei loro collaboratori.

Il provider esterno ha cura di raccogliere i dati relativi alla partecipazione ai vari programmi e di archivarli, rendendoli disponibili alle strutture interessate.

L’Organismo di Vigilanza verifica, anche attraverso i flussi informativi di cui è destinatario, lo stato di attuazione delle attività formative e ha facoltà di chiedere controlli periodici sul livello di conoscenza, da parte del Personale, del Decreto, del Modello e delle sue implicazioni operative.

CAPITOLO 7 GLI ILLECITI PRESUPPOSTO – AREE, ATTIVITÀ E RELATIVI PRINCIPI DI COMPORTAMENTO E DI CONTROLLO

7.1 Individuazione delle aree sensibili

L'art. 6, comma 2, del D. Lgs. 231/2001 prevede che il Modello debba "individuare le attività nel cui ambito possono essere commessi reati".

Sono state pertanto analizzate, come illustrato al paragrafo 2.4, le fattispecie di illeciti presupposto per le quali si applica il Decreto; con riferimento a ciascuna categoria dei medesimi sono state identificate nella Società le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati.

Per ciascuna di tali aree si sono quindi individuate le singole attività sensibili e qualificati i principi di controllo e di comportamento cui devono attenersi tutti coloro che vi operano.

Il Modello trova poi piena attuazione nella realtà dell'azienda attraverso il collegamento di ciascuna area e attività "sensibile" con le strutture aziendali coinvolte e con la gestione dei processi e della relativa normativa di riferimento.

I protocolli di seguito rappresentati ripercorrono in larga misura quelli della Capogruppo, alla luce delle seguenti considerazioni:

- la Società ha realizzato un elevato grado di esternalizzazione presso la Capogruppo delle funzioni aziendali;
- la Società ha fatto propria normativa, procedure e processi che regolano l'attività della Capogruppo, ove opportuno e per quanto applicabili;
- l'attività di Internal Auditing è svolta da Intesa Sanpaolo S.p.A. nell'esercizio della sua peculiare funzione della Capogruppo.

In considerazione di tutto quanto sopra, quando nei successivi protocolli si fa riferimento alle strutture e/o funzioni e/o unità organizzative della Società ovvero più genericamente al termine "struttura" o "struttura aziendale", si intende fare riferimento anche alle strutture e/o alle funzioni della Capogruppo, di altra Società del Gruppo ovvero di altro outsourcer esterno quando le attività sono svolte in outsourcing. Analogamente, quando si fa riferimento alla normativa interna, ci si riferisce anche alla normativa della Capogruppo recepita dalla Società.

Sulla base delle disposizioni di legge attualmente in vigore le aree sensibili identificate dal Modello riguardano in via generale:

- Area Sensibile concernente i reati contro la Pubblica Amministrazione e il reato di corruzione tra privati;
- Area Sensibile concernente i reati societari;
- Area sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali, i reati contro la persona, i reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa;
- Area sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio;
- Area Sensibile concernente i reati in tema di salute e sicurezza sul lavoro;

- Area Sensibile concernente i reati informatici e di indebito utilizzo di strumenti di pagamento diversi dai contanti;
- Area sensibile concernente i reati contro l'industria e il commercio, i reati in materia di violazione del diritto d'autore e i reati doganali;
- Area Sensibile concernente i reati ambientali;
- Area Sensibile concernente i reati tributari.

7.2 Area sensibile concernente i reati contro la Pubblica Amministrazione e il reato di corruzione tra privati

7.2.1 Fattispecie di reato

Premessa

Gli artt. 24 e 25 del Decreto contemplano una serie di reati previsti dal codice penale accomunati dall'identità del bene giuridico da essi tutelato, individuabile nell'imparzialità e nel buon andamento della Pubblica Amministrazione.

La costante attenzione del legislatore al contrasto della corruzione ha portato a ripetuti interventi in detta materia e nel corso del tempo sono state inasprite le pene e introdotti o, modificati alcuni reati, tra i quali il reato di "*Induzione indebita a dare o promettere utilità*", la cui condotta in precedenza era ricompresa nel reato di "*Concussione*", e il reato di "*Traffico di influenze illecite*". È stato anche previsto il reato di "*Corruzione tra privati*"; il D. Lgs. 38/2017 ha altresì introdotto il reato societario di "*Istigazione alla corruzione tra privati*" di cui all'articolo 2635-bis del Codice Civile. Tali reati, descritti nel paragrafo 7.3, pur essendo reati societari di cui all'articolo 25-ter, si collocano nel più ampio ambito delle misure di repressione dei fenomeni corruttivi che possono compromettere la leale concorrenza e il buon funzionamento del sistema economico in genere; risultano invero assimilabili, per modalità di compimento e per principi di controllo e comportamento che impattano sui medesimi, ai reati di "corruzione" di cui all'art. 25 del Decreto. Con la presente Area Sensibile, pertanto, si intende presidiare anche il rischio di commissione dei reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Inoltre, la Legge 09.01.2019 n. 3 "*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*" ha introdotto tra i reati presupposto altresì la fattispecie di "*Traffico di influenze illecite*" di cui all'art. 346-bis c.p. inserendola tra le ipotesi previste dall'art. 25 del Decreto 231/2001. In particolare, tale fattispecie punisce coloro i quali, al di fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter c.p. e nei reati di corruzione di cui all'articolo 322-bis c.p., sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis c.p., indebitamente facciano 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 un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis c.p., ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

Sono stati altresì aggiunti ulteriori reati posti a tutela delle pubbliche finanze, italiane e dell'Unione Europea, tra cui reati di "*Peculato*" e di "*Abuso d'ufficio*"⁶.

Agli effetti della legge penale si considera Ente della Pubblica Amministrazione qualsiasi persona giuridica che persegua e/o realizzi e gestisca interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa, disciplinata da norme di diritto pubblico e manifestantesi mediante atti autoritativi.

⁶ La possibilità di commissione dei reati di peculato e d'abuso di ufficio, tenuto conto dell'operatività della Società, è ritenuta ragionevolmente remota.

A titolo meramente esemplificativo ed avendo riguardo all'operatività della Società si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione: i) lo Stato, le Regioni, le Province, i Comuni; ii) i Ministeri, i Dipartimenti, le Commissioni; (iii) gli Enti Pubblici non economici (INPS, ENASARCO, INAIL, ISTAT); (iv) le ASL e le Agenzie delle Entrate.

Tra le fattispecie penali qui considerate, i reati di concussione e di induzione indebita a dare o promettere utilità nonché i reati di corruzione, nelle loro varie tipologie, presuppongono il coinvolgimento necessario di un soggetto privato e di un pubblico agente, vale a dire di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" e/o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p.

In sintesi, può dirsi che la distinzione tra le due figure è in molti casi controversa e labile e che la stessa è definita dalle predette norme secondo criteri basati sulla funzione oggettivamente svolta dai soggetti in questione.

La qualifica di Pubblico Ufficiale è attribuita a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. L'esercizio di una pubblica funzione amministrativa solitamente è riconosciuto sussistere in capo a coloro che formano o concorrono a formare la volontà dell'ente pubblico o comunque lo rappresentano di fronte ai terzi, nonché a coloro che sono muniti di poteri autoritativi o certificativi⁷.

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

La qualifica di Incaricato di Pubblico Servizio si determina per via di esclusione, spettando a coloro che svolgono quelle attività di interesse pubblico, non consistenti in semplici mansioni d'ordine o meramente materiali, disciplinate nelle stesse forme della pubblica funzione, ma alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale.

A titolo esemplificativo si elencano i seguenti soggetti nei quali la giurisprudenza ha individuato la qualifica di Incaricato di Pubblico Servizio: esattori dell'Enel, lettori dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento della corrispondenza, dipendenti del Poligrafico dello Stato, guardie giurate che conducono furgoni portavalori.

Va considerato che la legge non richiede necessariamente, ai fini del riconoscimento in capo ad un determinato soggetto delle qualifiche pubbliche predette, la sussistenza di un rapporto di impiego con un Ente pubblico: la pubblica funzione od il pubblico servizio possono essere esercitati, in casi particolari, anche da un privato (es.: notaio). Determinate attività potrebbero assumere, secondo la giurisprudenza, una connotazione di rilevanza pubblicistica tale da far riconoscere anche in capo ai dipendenti ed esponenti di un ente non pubblico, la qualifica di pubblico agente, ovvero di Incaricato

⁷ Rientra nel concetto di poteri autoritativi non solo il potere di coercizione ma ogni attività discrezionale svolta nei confronti di soggetti che si trovano su un piano *non paritetico* rispetto all'autorità (cfr. Cass., Sez. Un. 11/07/1992, n.181). I poteri certificativi comprendono tutte quelle attività di documentazione cui l'ordinamento assegna efficacia probatoria, quale che ne sia il grado.

di Pubblico Servizio. Pertanto, i dipendenti ed esponenti di un ente non pubblico che, nell'esercizio delle predette attività di rilevanza pubblica, pongono in essere le condotte tipiche dei pubblici agenti descritte nei reati di corruzione, concussione e induzione indebita a dare o promettere utilità sono puniti come tali e può inoltre scattare la responsabilità della Società ai sensi del D. Lgs. 231/2001. La responsabilità degli esponenti e dei dipendenti, nonché dell'ente, può altresì conseguire qualora essi tengano nei confronti di pubblici agenti le condotte tipiche dei soggetti privati descritte nei predetti reati.

Deve porsi particolare attenzione al fatto che, ai sensi dell'art. 322-*bis* c.p., la condotta del soggetto privato – sia esso corruttore o indotto a dare o promettere utilità – è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi delle Comunità Europee, o degli Enti costituiti sulla base dei Trattati che istituiscono le Comunità europee, o, infine, nell'ambito degli altri Stati membri dell'Unione europea; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, Assemblee parlamentari internazionali, Corti internazionali.

Si illustrano sinteticamente qui di seguito le fattispecie delittuose previste dagli artt. 24 e 25 del Decreto⁸. Per quanto riguarda le fattispecie previste dall'art. 25-*ter* del Decreto, si rimanda a quanto descritto nel Capitolo 7.3.

Peculato (art. 314, comma 1, e art. 316 c.p.)

Il reato è commesso dal pubblico ufficiale o dall'incaricato di pubblico servizio che si appropria di denaro o di beni mobili altrui di cui abbia per ragione di servizio il possesso o la disponibilità, oppure che riceve o trattiene indebitamente per sé o per terzi, denaro o altra utilità, percepiti approfittando dell'errore altrui.

Tali condotte comportano la responsabilità amministrativa ai sensi del D. Lgs. 231/2001 solo se i fatti offendano gli interessi finanziari dell'UE.

Si tratta di illeciti contestabili in situazioni in cui non ricorrano gli elementi di altri reati, quali ad esempio quello di truffa ai danni dell'UE.

Abuso d'ufficio (art. 323 c.p.)

La norma punisce qualsiasi condotta relativa alle funzioni del pubblico ufficiale o dell'incaricato di pubblico servizio che non ricada in specifiche fattispecie penali più gravi, ma che comunque sia connotata dall'intenzione di procurare a sé o ad altri un vantaggio patrimoniale ingiusto o arrecare ad altri un danno ingiusto. La condotta deve essere caratterizzata da:

- violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge, dalle quali non residuino margini di discrezionalità nelle decisioni;

⁸ Gli articoli 24 e 25 del D. Lgs. 231/2001 sono stati modificati dall'articolo 5 del D. Lgs. 75/2020 che, a far tempo dal 30 luglio 2020, ha introdotto i nuovi reati presupposto di peculato, di abuso d'ufficio, di frode nelle pubbliche forniture, di indebita percezione di erogazioni del Fondo europeo agricolo, di truffa e di frode informatica ai danni dell'UE.

- presenza di conflitto con un interesse proprio o di un prossimo congiunto o di altre situazioni che per legge impongano di astenersi dal compimento dell'atto.

Tali condotte comportano la responsabilità amministrativa ai sensi del D. Lgs. 231/2001 solo se i fatti offendano gli interessi finanziari dell'UE.

Malversazione di erogazioni pubbliche (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto in modo lecito contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, da parte dello Stato italiano, di altro ente pubblico o dell'UE destinati alla realizzazione di una o più finalità, non si proceda all'utilizzo delle somme per le finalità per cui sono state concesse.

Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.)

La fattispecie criminosa si realizza nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute – si ottengano, per sé o per altri e senza averne diritto, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dall'UE. A nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato si perfeziona nel momento dell'ottenimento delle erogazioni. La condotta è punita più severamente se lede interessi finanziari dell'UE e il danno o il profitto superano € 100 mila.

Indebita percezione di erogazioni del Fondo europeo agricolo (art. 2 L. n. 898/1986)

Tale disposizione punisce chiunque mediante l'esposizione di dati o notizie falsi ottiene per sé o per altri aiuti, premi, indennità, restituzioni o erogazioni in genere a carico, anche solo in parte, al Fondo europeo agricolo di garanzia o al Fondo europeo agricolo per lo sviluppo rurale. A tali erogazioni sono assimilate le quote nazionali complementari rispetto a quelle erogate dai predetti Fondi nonché le erogazioni poste a totale carico della finanza nazionale sulla base della normativa UE in materia. Quando la condotta non consista nella sola falsità delle informazioni, ma sia caratterizzata da artifici o raggiri di effettiva portata decettiva ricorre il più grave reato di truffa ai danni dello Stato.

Frode nelle pubbliche forniture (art. 356 c.p.)

Commette il reato chiunque nell'esecuzione di contratti di fornitura con lo Stato, con un altro ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità non adempia ai propri obblighi, facendo ricorso ad artifici o raggiri tali da ingannare la controparte sul contenuto della propria prestazione, facendo mancare in tutto o in parte cose o opere necessarie a uno stabilimento pubblico o a un servizio pubblico.

La pena è aumentata se la fornitura concerne sostanze alimentari o medicinali, ovvero cose od opere destinate alle comunicazioni, all'armamento o equipaggiamento delle forze armate, o ad ovviare a un comune pericolo o a un pubblico infortunio.

Truffa ai danni dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui si ottenga un ingiusto profitto ponendo in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato, ad altro ente pubblico, oppure all'UE.

Il reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni supportate da documentazione artefatta, al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni da parte dello Stato, di altro ente pubblico o dell'UE.

Gli elementi caratterizzanti il reato in esame sono: rispetto al reato di truffa generica (art. 640, comma 2, n. 1, c.p.), l'oggetto materiale specifico, che per la presente fattispecie consiste nell'ottenimento di erogazioni pubbliche comunque denominate; rispetto al reato di indebita percezione di erogazioni (art. 316-ter c.p.), la necessità dell'ulteriore elemento della attivazione di artifici o raggiri idonei ad indurre in errore l'ente erogante.

Frode informatica (art. 640-ter c.p.)

La fattispecie di frode informatica consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati, informazioni o programmi in essi contenuti, ottenendo un ingiusto profitto. Essa assume rilievo ai fini del Decreto, nel caso in cui sia perpetrata ai danni dello Stato, di altro ente pubblico o dell'UE ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale (sul punto cfr. par. 7.7.1).

In concreto, può integrarsi il reato ai danni della Pubblica Amministrazione o dell'UE qualora, ad esempio, una volta ottenuto un finanziamento, venisse violato un sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

Concussione (art. 317 c.p.)

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

La costrizione si attua mediante violenza o minaccia, esplicita o implicita, di un danno ingiusto (ad es.: rifiuto di compiere un atto dovuto se non contro compenso) da cui deriva una grave limitazione – senza annullarla del tutto – della libertà di autodeterminazione del destinatario che, senza alcun vantaggio indebito per sé, è posto nell'alternativa di subire il male prospettato o evitarlo attraverso la dazione o promessa dell'indebito. Per tale ragione il soggetto che subisce la costrizione è considerato vittima del reato e quindi esente da pena.

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

- condotta estorsiva posta in essere in concorso con un pubblico ufficiale o un incaricato di pubblico servizio nei confronti di un terzo;
- condotta estorsiva tenuta nell'esercizio di talune attività di rilevanza pubblica che, come illustrato in Premessa, possono comportare l'assunzione in capo al soggetto appartenente ad una società della qualifica di pubblico ufficiale o di incaricato di pubblico servizio.

Induzione indebita a dare o promettere utilità (art. 319-*quater* c.p.)

Il reato punisce la condotta dell'incaricato di pubblico servizio o del pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere a lui o a un terzo denaro o altre utilità non dovute.

Si tratta di fattispecie diversa da quella di concussione: le pressioni e richieste del pubblico agente non sono tali da esercitare la violenza morale tipica dell'estorsione, ma assumono forme di mero condizionamento della volontà della controparte, quali prospettazioni di possibili conseguenze sfavorevoli o difficoltà, ostruzionismi, eccetera. È punita anche la condotta della persona che cede all'induzione, corrispondendo o promettendo l'indebita utilità per evitare un danno o conseguire un vantaggio illecito. Tale condotta è punita più severamente se lede interessi finanziari dell'UE e il danno o il profitto superano € 100 mila.

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

- condotta induttiva posta in essere in concorso con un pubblico ufficiale o con un incaricato di pubblico servizio nei confronti di un terzo;
- condotta induttiva tenuta nell'esercizio di talune attività di rilevanza pubblica che, come illustrato in "Premessa", possono comportare l'assunzione in capo al soggetto appartenente ad una società della qualifica di pubblico ufficiale o di incaricato di pubblico servizio;
- accettazione delle condotte induttive provenienti da un pubblico ufficiale o da un incaricato di pubblico servizio.

Corruzione contro la Pubblica Amministrazione

L'elemento comune a tutte le varie fattispecie del reato di corruzione contro la Pubblica Amministrazione consiste nell'accordo fra un pubblico ufficiale o incaricato di pubblico servizio e un soggetto privato.

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

Nel fatto della corruzione si ravvisano due distinti reati: l'uno commesso dal soggetto corrotto, rivestente la qualifica pubblica (c.d. corruzione passiva), l'altro commesso dal corruttore (c.d. corruzione attiva) che, in forza della disposizione di cui all'art. 321 c.p. (Pene per il corruttore), è punito con le stesse pene previste per il corrotto.

Le fattispecie di corruzione previste dall'art. 25 del Decreto sono le seguenti.

Corruzione per l'esercizio della funzione (art. 318 c.p.)

Tale ipotesi di reato, si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio riceva, per sé o per o per un terzo, denaro o altra utilità, o ne accetti la promessa, per l'esercizio delle sue funzioni o dei suoi poteri. L'attività del pubblico ufficiale o dell'incaricato di pubblico servizio può estrinsecarsi in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), ma il reato sussiste anche, se l'utilità indebita è:

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

Rilevano quindi ipotesi di pericolo di asservimento della funzione ampie e sfumate e dazioni finalizzate a una generica aspettativa di trattamento favorevole⁹.

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Il reato, detto anche di "corruzione propria", consiste in un accordo per la promessa o dazione di un indebito compenso riferito ad un atto, da compiersi o già compiuto, contrario ai doveri del pubblico ufficiale o dell'incaricato di pubblico servizio (ad esempio: corresponsione di denaro per garantire l'aggiudicazione di una gara).

Corruzione in atti giudiziari (art. 319-ter, comma 1, c.p.)

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

Istigazione alla corruzione (art. 322 c.p.)

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

⁹ L'art. 318 c.p. previgente alla "legge anticorruzione" contemplava la sola ipotesi della cosiddetta "corruzione impropria", vale a dire l'indebito compenso per il compimento di uno specifico atto, dovuto o comunque conforme ai doveri d'ufficio, del pubblico agente. Il comma 2 prevedeva la condotta di "corruzione impropria susseguente", vale a dire l'indebito compenso non pattuito, ma corrisposto dopo il compimento di un atto d'ufficio, ipotesi in cui era punito il corrotto, ma non il corruttore. A seguito dell'abolizione di tale comma, anche la condotta predetta rientra nella formulazione del comma 1, con la conseguenza che ora sono puniti entrambi anche in tale caso (cfr. l'art. 321 c. p.). Infine, non ha più rilevanza la qualità di dipendente pubblico dell'incaricato di pubblico servizio, che era richiesta per la sussistenza del reato in questione.

Traffico di influenze illecite (art. 346-bis c.p.)¹⁰

Commette il reato chi, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di pubblico servizio – o con i soggetti che esercitano corrispondenti funzioni nell’ambito dell’Unione Europea, di Paesi terzi, di Organizzazioni o di Corti internazionali – indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso tali soggetti, ovvero per remunerarli in relazione all’esercizio delle loro funzioni. È punito allo stesso modo dell’intermediario anche il soggetto che con lui si accorda per l’effettuazione delle illecite influenze.

Sono previste aggravanti di pena per i casi in cui il “venditore” di relazioni influenti, vere o vantate, rivesta la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, o per i casi in cui si prefiguri un’influenza sull’esercizio di attività giudiziarie, oppure il fine di remunerare un pubblico ufficiale o un incaricato di pubblico servizio per il compimento di un atto contrario ai doveri d’ufficio o per l’omissione o il ritardo di un atto d’ufficio.

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

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

7.2.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere comportamenti illeciti nei rapporti con la Pubblica Amministrazione e/o condotte riconducibili alle fattispecie di reato di corruzione tra privati sono le seguenti:

1. Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione;
2. Gestione delle attività inerenti la richiesta di autorizzazioni o l’esecuzione di adempimenti verso la Pubblica Amministrazione;
3. Gestione dei finanziamenti pubblici;
4. Gestione dei contenziosi e degli accordi transattivi;
5. Gestione dei rapporti con le Autorità di Vigilanza;
6. Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
7. Gestione di omaggi, spese di rappresentanza e sponsorizzazioni;
8. Gestione del processo di selezione e assunzione del personale;

¹⁰ Il reato di traffico di influenze illecite è stato introdotto nel codice penale dalla L. n. 190/2012 e poi modificato dalla L. n. 3/2019, che lo ha aggiunto ai reati presupposto previsti dall’art. 25 del D. Lgs. 231/2001, con effetto dal 31.1.2019.

9. Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo;
10. Gestione dei rapporti con i Regolatori.

Con riferimento all'attività sensibile concernente la "Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo" si rimanda al protocollo 7.7.2.1. Si riportano qui di seguito i protocolli che dettano i principi di controllo ed i principi di comportamento applicabili alle altre sopraelencate attività sensibili e che si completano con la normativa aziendale di dettaglio che regola le attività medesime.

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalla Capogruppo e/o da *outsourcer* esterni.

7.2.2.1 Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione

Premessa

Il presente protocollo si applica a tutte le strutture della Società coinvolte in attività connesse alla stipula e gestione di rapporti contrattuali con le controparti, ivi inclusi eventuali terzi partecipati dallo Stato o da Enti della Pubblica Amministrazione o comunque appartenenti alla Pubblica Amministrazione aventi ad oggetto, in particolare la ricerca, la costituzione e la gestione di *partnership* scientifiche, tecnologiche, finanziarie, etc. finalizzate alla ricerca applicata, sviluppo, ingegnerizzazione e concessione in uso ai soci della Società di modelli di intelligenza artificiale (“algoritmi”) volti al contrasto del crimine finanziario.

Le attività inerenti la stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione, sono svolte anche in coordinamento e con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere.

Ai sensi del D. Lgs. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di “*Corruzione contro la pubblica Amministrazione*”, nelle loro varie tipologie, “*Traffico di influenze illecite*”¹¹, “*Induzione indebita a dare o a promettere utilità*”, “*Truffa ai danni dello Stato o di altro Ente pubblico*”, “*Peculato*”, “*Abuso d’ufficio*”, “*Frode nelle pubbliche forniture*”, nonché di “*Corruzione tra privati*” e “*Istigazione alla corruzione tra privati*”.

Sussiste altresì il rischio della commissione di reati di “*Contraffazione, alterazione o uso di marchi o di segni distintivi ovvero di brevetti, modelli e disegni di prodotti industriali*” (art. 473 c.p.) e “*Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale*” (art. 517 *ter* c.p.).

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di “*Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione*” concerne i seguenti ambiti:

- ricerca e costituzione di *partnership* scientifiche, tecnologiche, commerciali, etc. con aziende, istituti finanziari, enti e istituzioni pubbliche e private operanti nei settori della tecnologia, dell’innovazione digitale e dell’*Anti Financial Crime*, finalizzate allo svolgimento di attività di ricerca, sviluppo e ingegnerizzazione di modelli di intelligenza artificiale volti al contrasto del crimine finanziario (in breve *partner* pubblici e/o privati);
- stipula e gestione di contratti con i *partner* pubblici e/o privati;

¹¹ Si ricorda che, ai sensi dell’art. 322 *bis* c.p., la condotta del corruttore, istigatore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni o degli organi dell’UE, degli Enti costituiti sulla base dei Trattati che istituiscono l’UE, o, infine, nell’ambito degli altri Stati membri dell’UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

- sviluppo (anche tramite partner esterni), ingegnerizzazione e messa a disposizione di terzi o dei soci (ad esempio tramite concessione della licenza d'uso) di algoritmi "anti-frode";
- eventuale partecipazione a gare pubbliche per l'aggiudicazione di servizi connessi con le attività svolte attraverso la:
 - predisposizione e approvazione della documentazione e modulistica necessaria per la partecipazione ai bandi di gara;
 - presentazione delle domande di partecipazione ai bandi di gara all'Ente pubblico di riferimento;
 - predisposizione e approvazione della documentazione e modulistica necessaria per l'offerta commerciale agli Enti;
 - presentazione delle offerte tecniche ed economiche all'Ente pubblico di riferimento.

Le modalità operative per la gestione del processo possono essere disciplinate, in tutto o in parte, nell'ambito della normativa interna, e/o di Gruppo applicabile, sviluppata ed aggiornata a cura delle strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - i soggetti che esercitano poteri autorizzativi e/o negoziali ovvero di gestione degli obblighi di natura contrattuale nei confronti di *partner* (pubblici o privati) sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal responsabile della struttura di riferimento tramite delega interna, da conservare a cura della struttura medesima o sulla base delle deliberazioni assunte in seno agli Organi aziendali;
 - gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto da soggetti appositamente incaricati;
 - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa ed impegno, ivi incluse quelle nei confronti della Pubblica Amministrazione.
- Segregazione dei compiti tra i soggetti coinvolti nel processo di definizione e gestione degli accordi contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione. In particolare:
 - le attività di sviluppo commerciale sono gestite congiuntamente da più soggetti sulla base dei rispettivi ruoli e competenze;
 - la definizione dell'accordo è esclusivamente affidata responsabile della struttura aziendale competente in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati; l'atto formale della stipula del contratto avviene in base al vigente sistema dei poteri e delle deleghe;
 - le attività di gestione dei rapporti sono svolte da strutture diverse rispetto a quelle che gestiscono operativamente le attività di ricerca, sviluppo e ingegnerizzazione;
 - i soggetti deputati alla predisposizione della documentazione pre-contrattuale e contrattuale sono differenti da coloro che sottoscrivono la stessa;

- la gestione di eventuali brevetti/licenze d'uso è demandata al Responsabile della struttura aziendale competente con il supporto delle Funzioni di riferimento della Capogruppo ed eventualmente di uno studio legale specializzato;
- i soggetti deputati alla predisposizione della documentazione per la partecipazione a bandi di gara pubblica sono differenti da coloro che sottoscrivono la stessa.
- Attività di controllo:
 - la documentazione relativa alla stipula dei rapporti contrattuali viene sottoposta per il controllo al Direttore Generale in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati;
 - le strategie di ricerca, sviluppo e ingegnerizzazione degli algoritmi sono delineate dal Direttore Generale nel rispetto degli indirizzi strategici previsti per la Società e in coordinamento con le Strutture competenti e, in particolare, con lo Steering Committee che supporta il Consiglio di Amministrazione nel governo e coordinamento delle stesse iniziative di ricerca, sviluppo e ingegnerizzazione, anche tenuto conto dei pareri e delle proposte dello Scientific Advisory Board;
 - ogni nuova iniziativa deve essere sottoposta ad un processo preliminare strutturato e formalizzato di valutazione e approvazione;
 - la documentazione relativa alla stipula dei rapporti contrattuali è sottoposta per il controllo al Responsabile della Unità Organizzativa *owner* dell'iniziativa che si avvale, per la definizione delle nuove tipologie contrattuali, del contributo consulenziale delle competenti Funzioni della Capogruppo, anche ai fini di assicurare la coerenza della nuova iniziativa alle logiche di *business* e reputazionali del Gruppo e la conformità legale del contratto. Eventuali modifiche alle clausole contrattuali *standard* richieste dalla controparte in fase di negoziazione sono preventivamente verificate dalle Funzioni della Capogruppo competenti;
 - tutta la documentazione predisposta dalla Società per l'eventuale accesso a bandi di gara pubblici deve essere verificata, in termini di veridicità e congruità sostanziale e formale, dal responsabile della Struttura aziendale competente in virtù dell'oggetto del contratto o da soggetti a ciò facoltizzati;
 - l'attività di ricerca e le relazioni con eventuali *partner* commerciali sono gestite dalle Unità Organizzative competenti, in accordo con il Direttore Generale;
 - prima di stipulare accordi di *partnership* con una controparte terza, l'Unità competente, con il supporto delle Funzioni di riferimento della Capogruppo, effettua un'attività di *due diligence*, con particolare riguardo a quanto previsto dalle Linee Guida Anticorruzione di Gruppo;
 - gli accordi di *partnership* sono predisposti dall'Unità competente in coordinamento con le Funzioni interessate della Capogruppo;
 - dovrà essere garantita la previsione di specifiche procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge e contrattuali;
 - l'eventuale valutazione di brevettabilità (includere le ricerche di anteriorità volte a garantirne l'originalità e l'assenza di diritti altrui) di ogni nuova invenzione/innovazione sviluppata, nonché la preparazione ed il deposito della relativa domanda di brevetto, devono essere curati dalla

Unità competente con il supporto delle Funzioni della Capogruppo competenti e di uno studio legale specializzato in materia, a cui sia stato conferito un incarico scritto.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - ciascuna fase rilevante del processo deve risultare da apposita documentazione scritta;
 - ogni accordo/convenzione/contratto con le controparti è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
 - le relazioni di *business*, anche potenziali, più significative, vengono tracciate e condivise con il Direttore Generale e/o il Responsabile della Unità *owner* dell'iniziativa;
 - tutti gli accordi contrattuali vengono censiti dalla Struttura competente in apposita reportistica interna riportante, per ogni rapporto, le principali informazioni relative alla natura dello stesso e all'eventuale *partner* coinvolto;
 - la realizzazione delle operazioni nella esecuzione degli adempimenti contrattuali verso le controparti prevede l'utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate. Le Strutture Organizzative provvedono alla archiviazione della documentazione cartacea inerente all'esecuzione degli adempimenti svolti;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Società è responsabile dell'archiviazione e della conservazione della documentazione di competenza, relativa anche alle singole operazioni, prodotta anche in via telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula e gestione di rapporti con la clientela.
- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

La Società, nelle attività di stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione, è tenuta ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento e delle Linee Guida Anticorruzione di Gruppo. In particolare:

- tutti i soggetti che, nell'ambito del processo in oggetto, intrattengono rapporti contrattuali con rilevanza all'esterno della Società stessa, ivi inclusi quelli con la Pubblica Amministrazione, devono essere individuati ed autorizzati in base allo specifico ruolo attribuito loro dal sistema di poteri e deleghe vigente o dalla normativa interna;
- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con le controparti, inclusi i contratti di *partnership*, devono essere appositamente incaricati;

- il Personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1. ed al Responsabile Aziendale Anticorruzione;
- la corresponsione di onorari o compensi ad eventuali collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dal Direttore Generale o dalla Unità Organizzativa da questi delegata sulla base del vigente sistema di poteri e deleghe, competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.
- i contratti con i partner e con eventuali soggetti terzi coinvolti nella stipula dei relativi rapporti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;
- I contratti stipulati con i partner tecnologici devono prevedere apposita clausola di manleva della Società da eventuali responsabilità sull'eventuale lesione di diritti d'autore/licenze d'uso/brevetti di terzi.

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati e/o omettere informazioni rilevanti sulle caratteristiche delle singole operazioni;
- tenere una condotta ingannevole che possa indurre le controparti (pubbliche e private) in errore;
- chiedere o indurre – anche a mezzo di intermediari – gli esponenti apicali e/o persone loro subordinate di società controparti o in relazione con la Società, ivi inclusi funzionari della Pubblica Amministrazione, a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di stipulare accordi/convenzioni/contratti con la Società, nonché la gestione dei rapporti con la stessa;
- promettere o versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a esponenti apicali, e/o persone loro subordinate, di società controparti o in relazione con la Società, ivi inclusi funzionari della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della Società stessa. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione a favore di soggetti collegati, oppure la corresponsione di incentivi in violazione della disciplina di riferimento e della normativa aziendale oppure, più in generale, tutte le operazioni che comportino la generazione di una perdita per la Società e la creazione di un utile per i soggetti predetti;
- promettere versare/offrire somme di denaro non dovute, doni o gratuite prestazioni, vantaggi di qualsiasi natura, come descritti al punto precedente, a favore di esponenti apicali o di persone a

loro subordinate appartenenti a società/enti privati partecipanti a gare pubbliche al fine di dissuaderli dalla partecipazione o per conoscere le loro offerte e formulare le proprie in modo tale da ottenere l'aggiudicazione della gara, oppure minacciarli di un danno ingiusto per le medesime motivazioni;

- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico, dal Codice Interno di Comportamento di Gruppo e dalle Linee Guida Anticorruzione di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione, nelle loro varie tipologie, di *“Induzione indebita a dare o promettere utilità”*, *“Traffico di influenze illecite”*¹², nonché di *“Corruzione tra privati”* e di *“Istigazione alla corruzione tra privati”*, che potrebbe derivare dall'eventuale scelta di soggetti “vicini” a persone legate alla Pubblica Amministrazione ovvero a esponenti apicali o a persone a loro subordinate appartenenti a società private e dalla conseguente possibilità di agevolare l'instaurazione/sviluppo di rapporti finalizzati alla negoziazione e alla successiva gestione del rapporto contrattuale.

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

¹² Si ricorda che, ai sensi dell'art. 322 *bis* c.p., la condotta del corruttore, istigatore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, degli Enti costituiti sulla base dei Trattati che istituiscono l'UE, o, infine, nell'ambito degli altri Stati membri dell'UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

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

Premessa

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

- gestione dei rapporti con gli Enti assistenziali e previdenziali e realizzazione, nei tempi e nei modi previsti, degli adempimenti di legge in materia di lavoro e previdenza (INPS, INAIL, Direzione Provinciale del Lavoro, Medicina del Lavoro, Agenzia delle Entrate, Enti pubblici locali, ecc), anche ai fini della gestione delle categorie protette;
- gestione dei rapporti con le Camere di Commercio per l'esecuzione delle attività inerenti al registro delle imprese;
- gestione dei rapporti con gli Enti Locali territorialmente competenti in materia di smaltimento rifiuti;
- gestione dei rapporti con Amministrazioni Statali, Regionali, Comunali o Enti locali (ASL, Vigili del Fuoco, Arpa, etc.) intrattenuti, a titolo esemplificativo e non esaustivo, per l'esecuzione di adempimenti in materia di igiene e sicurezza e/o di autorizzazioni (ad esempio pratiche edilizie), permessi, concessioni;
- gestione dei rapporti con il Ministero dell'Economia e delle Finanze, con l'Agenzia Dogane e Monopoli, con le Agenzie Fiscali e con gli Enti pubblici locali per l'esecuzione di adempimenti in materia di imposte;
- gestione dei rapporti con la Prefettura, la Procura della Repubblica e le Camere di Commercio e/o l'Agenzia delle Entrate competenti per la richiesta di certificati e autorizzazioni.

Le attività inerenti alla richiesta di autorizzazioni o all'esecuzione di adempimenti verso la Pubblica Amministrazione sono svolte con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere.

Ai sensi del D. Lgs. 231/2001, le predette attività potrebbero presentare occasioni per la commissione dei reati di *“Corruzione contro la Pubblica Amministrazione”*, nelle loro varie tipologie, *“Induzione indebita a dare o promettere utilità”*, *“Traffico di influenze illecite”*¹³; *“Truffa ai danni dello Stato o di altro Ente Pubblico”*, *“Favoreggiamento personale”* e dei *Reati di contrabbando*¹⁴.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

¹³ Si ricorda che, ai sensi dell'art. 322 *bis* c.p., la condotta del corruttore, istigatore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, degli Enti costituiti sulla base dei Trattati che istituiscono l'UE, o, infine, nell'ambito degli altri Stati membri dell'UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

¹⁴ La possibilità di commissione dei reati di contrabbando, tenuto conto dell'operatività della Società, è stata ritenuta ragionevolmente remota.

Descrizione del Processo

Il processo di gestione dei rapporti con la Pubblica Amministrazione in occasione di richieste di autorizzazioni o esecuzione di adempimenti si articola nelle seguenti fasi, effettuate sotto la responsabilità delle Unità Organizzative competenti per materia:

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

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna e/o di Gruppo applicabile, sviluppata ed aggiornata a cura delle Unità Organizzative, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione delle attività inerenti alla richiesta di autorizzazioni, licenze, permessi, concessioni, alla Pubblica Amministrazione sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal vigente sistema di poteri e deleghe e dalla normativa interna; nel caso in cui i rapporti con gli Enti pubblici vengano intrattenuti da soggetti terzi, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali;
 - la gestione dei rapporti con i Pubblici Ufficiali, gli Incaricati di Pubblico Servizio e i rappresentanti della Pubblica Amministrazione in generale, in caso di accertamenti/sopralluoghi è attribuita ai soggetti appositamente incaricati ai sensi del sistema dei poteri e delle deleghe. Qualora i rapporti con esponenti della Pubblica Amministrazione siano intrattenuti da soggetti terzi – che operano in nome o per conto della Società – questi ultimi sono individuati con lettera di incarico/nomina ovvero nell'ambito dei contratti stipulati dalla Società, nei limiti della normativa applicabile e secondo le modalità dalla stessa previste.
- Segregazione dei compiti tra i soggetti coinvolti nel processo di gestione delle attività inerenti alla richiesta di autorizzazioni, o all'esecuzione di adempimenti verso la Pubblica Amministrazione al fine di garantire, per tutte le fasi del processo un meccanismo di *maker e checker*.
- Attività di controllo: le attività devono essere svolte in modo tale da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell'istanza di autorizzazione, alla richiesta di licenza, permesso o concessione o forniti in esecuzione degli adempimenti, prevedendo, ove opportuno, specifici controlli in contraddittorio. In particolare, laddove l'autorizzazione/adempimento preveda l'elaborazione di dati ai fini della

predisposizione dei documenti richiesti dall'Ente pubblico, è effettuato un controllo sulla correttezza delle elaborazioni da parte di soggetti diversi da quelli deputati alla esecuzione delle attività.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - copia della documentazione consegnata all'Ente pubblico per la richiesta di autorizzazione o per l'esecuzione di adempimenti è conservata presso l'archivio della Unità Organizzativa di competenza;
 - il Responsabile della struttura interessata dall'accertamento/sopralluogo, ovvero il soggetto aziendale all'uopo incaricato ha l'obbligo di firmare per accettazione il verbale redatto dai Funzionari pubblici in occasione degli accertamenti/sopralluoghi condotti presso la Società e di mantenerne copia nei propri uffici, unitamente ai relativi allegati;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Unità Organizzativa di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla richiesta di autorizzazioni alla Pubblica Amministrazione.

Principi di comportamento

Le Unità Organizzative, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione in occasione di richiesta di autorizzazioni o esecuzione di adempimenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati;
- il Personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1. ed al Responsabile Aziendale Anticorruzione;
- qualora sia previsto il coinvolgimento di soggetti terzi (professionisti, ditte, ecc.) nell'espletamento delle attività inerenti alla richiesta di autorizzazioni ovvero nell'esecuzione di adempimenti verso la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dal Consiglio di Amministrazione o dalla Unità Organizzativa, da questi delegata sulla base del vigente sistema di poteri e deleghe, e competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non

è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;

- nell'ambito delle ispezioni effettuate da parte dei Funzionari della Pubblica Amministrazione presso la sede della Società, fatte salve le situazioni in cui i Funzionari richiedano colloqui diretti con personale della Società specificamente individuato, partecipano agli incontri con i Funzionari stessi almeno due soggetti, se appartenenti alla funzione interessata dall'ispezione; diversamente, laddove l'ispezione sia seguita da funzioni diverse da quella coinvolta dalla verifica è prevista la partecipazione di un unico soggetto agli incontri con i Funzionari.

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

- ritardare senza giusto motivo o omettere l'esibizione di documenti/la comunicazione di dati richiesti;
- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- chiedere o indurre – anche a mezzo di intermediari – i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente il riscontro da parte della Pubblica Amministrazione;
- promettere o versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni o gratuite prestazioni al di fuori delle prassi dei regali di cortesia di modico valore e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi di AFC Digital HUB. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione a favore di soggetti collegati e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la Società e la creazione di un utile per i soggetti predetti;
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico, dal Codice Interno di Comportamento di Gruppo e dalle Linee Guida Anticorruzione di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione, nelle loro varie tipologie, di *“Induzione indebita a dare o promettere utilità”* e di *“Traffico di influenze illecite”*, che potrebbe derivare dall'eventuale scelta di soggetti “vicini” a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto con la Società.

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

7.2.2.3 Gestione dei finanziamenti pubblici

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative coinvolte nella richiesta e gestione di finanziamenti pubblici (ad esempio partecipazione a bandi pubblici italiani ed europei per finanziare progetti di investimento, di ricerca e sviluppo; richiesta e ricorso a finanziamenti, sovvenzioni e contributi per la formazione concessi da soggetti pubblici nazionali ed esteri).

Le attività inerenti alla gestione di finanziamenti pubblici sono svolte, ove applicabile (ad esempio in materia di formazione finanziata) con il supporto delle strutture competenti della Capogruppo.

Ai sensi del D. Lgs. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di *“Corruzione contro la Pubblica Amministrazione”* nelle loro varie tipologie, *“Induzione indebita a dare o promettere utilità”*, *“Traffico di influenze illecite”*¹⁵, *“Truffa ai danni dello Stato o di altro Ente pubblico”*, *“Truffa aggravata per il conseguimento di erogazioni pubbliche”*, *“Malversazione di erogazioni pubbliche”*, *“Indebita percezione di erogazioni a danno dello Stato”*, *“Peculato”* e *“Abuso d’ufficio”*.

Si rileva come i principi di controllo e di comportamento definiti nell’ambito del presente protocollo, conformi, ove applicabili e tenendo conto delle specificità organizzative e operative della Società, a quelli adottati dalla Capogruppo, risultano applicati sia a presidio delle attività svolte all’interno della Società, sia a presidio di tutte le attività esternalizzate alla Capogruppo sulla scorta del relativo contratto di servizio.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Descrizione del processo

L’eventuale processo di gestione dei finanziamenti pubblici si articola nelle seguenti fasi:

- individuazione delle iniziative finanziabili;
- predisposizione e presentazione della richiesta di finanziamento/contributo all’Ente Pubblico / partecipazione al bando di gara per l’ottenimento del finanziamento;
- attuazione dei progetti finanziati;
 - gestione dell’operatività dell’iniziativa finanziata;
 - gestione delle risorse previste dal progetto/iniziativa (economiche e tecniche, interne ed esterne);
- rendicontazione dei costi;
 - raccolta dei dati contabili, elaborazione e stesura di *report*;

¹⁵ Si ricorda che, ai sensi dell’art. 322-*bis* c.p., la condotta del corruttore, istigatore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni o degli organi dell’UE, degli Enti costituiti sulla base dei Trattati che istituiscono l’UE, o, infine, nell’ambito degli altri Stati membri dell’UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

- gestione dei rapporti con Enti in occasione di verifiche e ispezioni da parte dell'Ente finanziatore;
- gestione dell'introito del contributo.

Le modalità operative per la gestione del processo sono disciplinate nell'ambito della normativa interna e/o di Gruppo applicabile, sviluppata ed aggiornata a cura delle Unità Organizzative, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - i soggetti che, nell'ambito della "gestione dei finanziamenti pubblici", esercitano poteri autorizzativi e/o negoziali nei rapporti con gli Enti finanziatori sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile dell'Unità Organizzativa di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
 - le richieste di finanziamento/contributo sono sottoscritte dal Responsabile dell'Unità Organizzativa competente specificamente e formalmente facoltizzato in virtù del vigente sistema dei poteri e delle deleghe;
 - in caso di eventuale ricorso a consulenti esterni, il processo di attribuzione dell'incarico avviene uniformemente a quanto previsto dalle disposizioni contenute nella specifica sezione dedicata nel presente Modello (protocollo "Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali" di cui al paragrafo 7.2.2.6). La selezione di tali consulenti avviene in ogni caso prevedendo l'acquisizione di una pluralità di offerte e la scelta mediante criteri oggettivi e codificati.
- Segregazione dei compiti tra i differenti soggetti coinvolti, volta a garantire, per tutte le fasi del processo, un meccanismo di *maker e checker*.
- Attività di controllo da parte di ciascuna Struttura competente ed in particolare:
 - verifica della coerenza dei contenuti del progetto della Società rispetto a quanto disposto dalle direttive del bando di finanziamento;
 - verifica della regolarità formale della documentazione da consegnare all'Ente per l'accesso al bando di finanziamento;
 - tenuta, con riferimento alla formazione finanziata, del registro presenze durante l'erogazione dei progetti formativi e utilizzo di sistemi informatici di supporto per la gestione del personale, in cui sono registrate tutte le informazioni relative alle presenze, agli allontanamenti ed alle attività svolte;
 - puntuale attività di controllo sul processo di rendicontazione delle spese, attraverso:
 - raccolta e verifica della documentazione relativa all'iniziativa finanziata da presentare all'Ente finanziatore (in caso di formazione finanziata, raccolta e verifica dei registri di

presenza compilati in ogni loro parte dai partecipanti agli interventi formativi e raccolta della documentazione degli oneri aziendali dei dipendenti partecipanti/ docenti);

- raccolta e verifica delle parcelle/fatture relative ai costi sostenuti per l'iniziativa;
- verifica sulla puntuale e corretta contabilizzazione degli introiti.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - tutte le fasi di processo sono documentate, così come previsto dagli stessi bandi per l'ottenimento dei finanziamenti. In particolare, ciascuna Struttura coinvolta è responsabile dell'archiviazione e della conservazione della documentazione di propria competenza, ivi inclusa quella trasmessa all'Ente finanziatore pubblico anche in via telematica o elettronica.

Principi di comportamento

Le Unità Organizzative, a qualsiasi titolo coinvolte nella attività di gestione dei finanziamenti pubblici, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

In particolare:

- tutti i soggetti che, in fase di richiesta e gestione dei finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della Società devono essere espressamente autorizzati;
- gli esponenti e il Personale coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società (es.: pratiche di richiesta, studi di fattibilità, piani di progetto, ecc.) devono essere appositamente incaricati;
- gli esponenti e il Personale non possono dare seguito a qualunque richiesta di indebiti vantaggi, denaro o altra utilità o tentativi di corruzione da parte di un funzionario della Pubblica Amministrazione di cui dovessero essere destinatari o venirne semplicemente a conoscenza e devono immediatamente segnalarla all'Organismo di Vigilanza secondo le modalità previste dal paragrafo 4.1 ed al Responsabile Aziendale Anticorruzione;
- qualora sia previsto il coinvolgimento di soggetti terzi nella predisposizione delle pratiche di richiesta / gestione del finanziamento o nella successiva esecuzione di attività connesse con i programmi finanziati, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs.

231/2001, o disposizioni di legge contro la corruzione e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi e alterati;
- tenere una condotta ingannevole che possa indurre gli Enti finanziatori / erogatori in errore di valutazione tecnico-economica della documentazione presentata;
- chiedere o indurre – anche a mezzo di intermediari – i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di accoglimento delle domande di ammissione al contributo;
- destinare contributi, sovvenzioni, finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti;
- promettere o versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a favore di esponenti/rappresentanti della Pubblica Amministrazione o di Enti finanziatori, con la finalità di promuovere o favorire interessi della Società;
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico, dal Codice Interno di Comportamento di Gruppo e dalle Linee Guida Anticorruzione di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione nelle loro varie tipologie, e di *“Induzione indebita”*, di *“Traffico di Influenze illecite”* e del reato di *“Corruzione tra privati”* che potrebbe derivare dall'eventuale scelta di soggetti “vicini” a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di facilitare/velocizzare l'iter istruttorio delle pratiche.

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

7.2.2.4 Gestione dei contenziosi e degli accordi transattivi

Premessa

Attualmente, la Società, anche in considerazione della propria operatività, non gestisce contenziosi giudiziali o stragiudiziali (di natura amministrativa, civile, penale, fiscale, giuslavoristica e previdenziale) o accordi transattivi né con Enti pubblici né con soggetti privati.

Tuttavia, nel caso in cui in futuro la Società si dovesse trovare nella necessità di gestire, anche occasionalmente, tale attività, le strutture coinvolte dovranno assicurare il rispetto della normativa di Gruppo applicabile nonché delle regole definite dal presente protocollo.

Ai sensi del D. Lgs. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di *“Corruzione contro la Pubblica Amministrazione”*, nelle loro varie tipologie¹⁶, *“Induzione indebita a dare o promettere utilità”*, *“Traffico di influenze illecite”*¹⁷, *“Truffa ai danni dello Stato o di altro Ente Pubblico”*, *“Corruzione tra privati”*, *“Istigazione alla corruzione tra privati”*, nonché del reato di *“Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria”*¹⁸ che si intende presidiare attraverso il presente protocollo.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Descrizione del Processo

Gestione dell’eventuale contenzioso

Il processo di gestione dell’eventuale contenzioso si articola nelle seguenti fasi, effettuate sotto la responsabilità del Presidente del Consiglio di Amministrazione o del Direttore Generale – nei limiti delle attribuzioni delegate e dei poteri ad essi conferiti dal C.d.A., in coordinamento con l’Unità Organizzativa interessata dalla controversia e con il supporto degli eventuali professionisti esterni incaricati:

- apertura del contenzioso giudiziale o stragiudiziale;
 - raccolta delle informazioni e della documentazione relative alla vertenza;
 - analisi, valutazione e produzione degli elementi probatori;
 - predisposizione degli scritti difensivi e successive integrazioni, direttamente o in collaborazione con i professionisti esterni;

¹⁶ Ivi compresa la “corruzione in atti giudiziari” (art. 319-ter comma 1, c.p.).

¹⁷ Si ricorda che, ai sensi dell’art. 322 bis c.p., la condotta del corruttore, istigatore o del soggetto che cede all’induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell’ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito delle Istituzioni o degli organi dell’UE, degli Enti costituiti sulla base dei Trattati che istituiscono l’UE, o, infine, nell’ambito degli altri Stati membri dell’UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell’ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

¹⁸ Tale reato, punito dall’art. 377-bis c.p., costituisce reato presupposto della responsabilità degli enti ai sensi dell’art. 25-decies del Decreto. Inoltre, ai sensi dell’art. 10 della L. n.146/2006 può dar luogo alla medesima responsabilità anche se commesso in forma transnazionale. Si considera reato 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”.

- gestione della vertenza;
- ricezione, analisi e valutazione degli atti relativi alla vertenza;
- predisposizione dei fascicoli documentali;
- partecipazione, ove utile o necessario, alla causa, in caso di contenzioso giudiziale;
- intrattenimento di rapporti costanti con gli eventuali professionisti incaricati, individuati nell'ambito dell'apposito albo;
- assunzione delle delibere per:
 - determinazioni degli stanziamenti al Fondo Rischi e Oneri in relazione delle vertenze passive e segnalazione dell'evento quale rischio operativo;
 - esborsi e transazioni;
- chiusura della vertenza.

Gestione degli accordi transattivi

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

Il processo si articola nelle seguenti fasi:

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

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

Principi di controllo

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

- Livelli autorizzativi definiti: la gestione dei contenziosi e degli accordi transattivi, inclusi quelli con la Pubblica Amministrazione prevede l'accentramento delle responsabilità di indirizzo e/o gestione e monitoraggio delle singole fasi del processo in capo al Presidente e/o Direttore Generale ovvero alle competenti funzioni a seconda della natura dei profili giuridici. Sono inoltre previsti, nell'ambito di ciascuna fase operativa caratteristica del processo, i seguenti presidi:
 - il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni, nonché le facoltà di autonomia per la gestione del contenzioso, ivi incluso quello nei confronti della Pubblica Amministrazione;
 - il conferimento degli incarichi a legali esterni, diversi da quelli individuati nell'ambito dell'albo predisposto e approvato dall'Unità Organizzativa competente, è autorizzato ai sensi del vigente sistema dei poteri e delle deleghe.

- Segregazione dei compiti: attraverso il chiaro e formalizzato conferimento di compiti e responsabilità nell'esercizio delle facoltà assegnate nello svolgimento delle attività di cui alla gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione.
- Attività di controllo:
 - rilevazione e monitoraggio periodico delle vertenze pendenti;
 - verifica periodica della regolarità, della completezza e correttezza di tutti gli adempimenti connessi a vertenze/transazioni che devono essere supportati da meccanismi di *maker* e *checker*.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - ciascuna fase rilevante del processo deve risultare da apposita documentazione scritta;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Unità Organizzativa di volta in volta interessata è altresì responsabile dell'archiviazione e della conservazione della documentazione di competenza anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione dei contenziosi e degli accordi transattivi ivi inclusi quelli con la Pubblica Amministrazione.

Principi di comportamento

Le Unità Organizzative a qualsiasi titolo coinvolte nella gestione degli eventuali contenziosi e accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

In particolare:

- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla Società devono essere appositamente incaricati;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del contenzioso e degli accordi transattivi, i contratti/lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dal Presidente o dal Direttore Generale oppure dalla Unità Organizzativa da questi delegata, al fine di valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- il Personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere

destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1 ed al Responsabile Aziendale Anticorruzione.

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

- in sede di contatti formali od informali, o nel corso di tutte le fasi del procedimento:
 - avanzare indebite richieste o esercitare pressioni su Giudici o Membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio);
 - indurre chiunque al superamento di vincoli o criticità ai fini della tutela degli interessi della Società;
 - indurre – con violenza o minaccia o, alternativamente, con offerta o promessa di denaro o di altra utilità – a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;
 - influenzare indebitamente le decisioni dell'Organo giudicante o le posizioni della Pubblica Amministrazione, quando questa sia controparte del contenzioso/arbitrato;
- in occasione di ispezioni/controlli/verifiche influenzare il giudizio, il parere, il rapporto o il referto degli Organismi pubblici o nominati dall'Organo giudicante o della Polizia giudiziaria;
- chiedere o indurre – anche a mezzo di intermediari – esponenti apicali e/o persone loro subordinate di società controparti o in relazione con la Società, ivi inclusi soggetti della Pubblica Amministrazione, a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Società;
- riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- promettere versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni o gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), o accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la Società, ivi inclusi soggetti della Pubblica Amministrazione, al fine di favorire indebitamente gli interessi della Società stessa, oppure minacciarli di un danno ingiusto per le medesime motivazioni. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione a favore di soggetti collegati, la corresponsione di incentivi in violazione della disciplina di riferimento e della normativa aziendale e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la Società e la creazione di un utile per i soggetti predetti;
- affidare incarichi a professionisti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del professionista devono ispirarsi ai criteri di

chiarezza e documentabilità dettati dal Codice Etico, dal Codice Interno di Comportamento di Gruppo e dalle Linee Guida Anticorruzione di Gruppo; ciò al fine di prevenire il rischio di commissione del reato di corruzione nelle loro varie tipologie, compresa la *“Corruzione tra privati”* e l’*“Istigazione alla corruzione tra privati”*, e di *“Induzione indebita a dare o promettere utilità”* e di *“Traffico di influenze illecite”*, che potrebbe derivare dall’eventuale scelta di soggetti “vicini” a persone legate alla Pubblica Amministrazione ovvero a esponenti apicali o a persone a loro subordinate appartenenti a società private e dalla conseguente possibilità di agevolare/condizionare il rapporto con la Società.

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

7.2.2.5 Gestione dei rapporti con le Autorità di Vigilanza

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative coinvolte nella gestione dei rapporti con le Autorità di Vigilanza e riguarda qualsiasi tipologia di attività posta in essere in occasione di eventuali adempimenti, comunicazioni, richieste e visite ispettive.

Le attività inerenti all'eventuale gestione dei rapporti con le Autorità di Vigilanza sono svolte con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere, in base al quale la Capogruppo ha mandato per operare in nome e per conto della Società nei confronti di organi o autorità di vigilanza.

Ai sensi del D. Lgs. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di *“Corruzione contro la Pubblica Amministrazione”*, nelle loro varie tipologie, *“Induzione indebita a dare o promettere utilità”*, *“Traffico di influenze illecite”*¹⁹ e *“Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza”* (art. 2638 del codice civile), di cui all'art. 25 *ter* del D. Lgs. 231/2001, annoverato fra i reati societari e descritto nel presente Modello nell'ambito nella specifica *“Area Sensibile concernente i reati societari”*.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti con le Autorità di Vigilanza quali, a titolo esemplificativo e non esaustivo:

- Garante per la protezione dei dati personali;
- Autorità di Supervisione in materia fiscale (Agenzia delle Entrate);
- Banca d'Italia;
- Banca Centrale Europea.

I principi di comportamento contenuti nel presente protocollo si applicano, a livello d'indirizzo comportamentale, anche nei confronti delle Autorità di Vigilanza estere²⁰.

Descrizione del Processo

Le attività inerenti alla gestione dei rapporti con le Autorità di Vigilanza sono riconducibili alle seguenti tipologie:

- richieste/istanze di abilitazioni, autorizzazioni, e/o informative/dati.
- riscontri ed adempimenti connessi a richieste/istanze delle Autorità di Vigilanza;
- gestione dei rapporti con i funzionari delle Autorità di Vigilanza in occasione di visite ispettive;

¹⁹ Si ricorda che, ai sensi dell'art. 322 *bis* c.p., la condotta del corruttore, istigatore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, degli Enti costituiti sulla base dei Trattati che istituiscono l'UE, o, infine, nell'ambito degli altri Stati membri dell'UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

²⁰ Si osserva che la Società non è sottoposta alla vigilanza di Autorità quali ad esempio la Banca Centrale Europea e la Banca d'Italia per via della natura non bancaria e finanziaria dell'attività attualmente svolta. Tuttavia, considerata l'appartenenza al Gruppo Intesa Sanpaolo, si precisa che i principi di comportamento contenuti nel presente protocollo risultano applicabili, a livello di indirizzo comportamentale, anche nei confronti delle suddette Autorità.

- monitoraggio delle azioni di *remediation* e rendicontazione / informativa all’Autorità di Vigilanza attraverso la predisposizione periodica di *report* sintetici.

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

Si rappresenta, a questo riguardo che le “Regole di Gruppo per la gestione dei rapporti con i Supervisor e le Autorità di Regolamentazione” individuano le strutture tenute ad assicurare il coordinamento delle comunicazioni con le Autorità e la coerenza trasversale delle stesse a livello di Gruppo (c.d. Struttura Pivot).

In ragione dell’oggetto/ambito del singolo contatto o della singola tematica, la struttura Pivot ingaggia le strutture responsabili (c.d. “Owner Funzionali”) per aspetti e contributi specifici per gli ambiti di competenza di volta in volta individuati.

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - ad eccezione delle visite ispettive, i rapporti con le Autorità di Vigilanza sono intrattenuti dai soggetti all’uopo delegati;
 - gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto da soggetti incaricati;
 - il riscontro ai rilievi delle Autorità è sottoposto, laddove previsto, all’approvazione e/o esame dei Comitati endoconsiliari competenti della Capogruppo ed al Consiglio di Amministrazione.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con le Autorità di Vigilanza. In particolare:
 - con riferimento alla gestione dei rapporti non riconducibili alla ordinaria operatività delle strutture della Società, tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell’operatività aziendale indirizzata alle Autorità di Vigilanza è redatta dalla Struttura Pivot con il supporto dell’*Owner* funzionale.
 - con riferimento alle visite ispettive la Struttura Pivot, avuta notizia dell’ispezione, avvisa la funzione Internal Auditing della Capogruppo, il Direttore Generale della Società ed i Responsabili delle Unità Organizzative interessate dalla visita ispettiva che, dopo aver accertato l’oggetto dell’ispezione, individuano le risorse deputate a gestire i rapporti con i funzionari pubblici durante la loro permanenza presso la Società. Nei casi particolarmente rilevanti, l’Organismo di Vigilanza deve essere tempestivamente informato della visita ispettiva in atto e di eventuali prescrizioni o eccezioni rilevate dall’Autorità.
- Attività di controllo:

- controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle Autorità di Vigilanza da parte della Unità Organizzativa interessata per le attività di competenza, che devono essere supportate da meccanismi di *maker e checker*;
- controlli di carattere giuridico sulla conformità alla normativa di riferimento della comunicazione richiesta.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - è fatto obbligo a tutte le Unità Organizzative, a vario titolo coinvolte nella predisposizione e trasmissione di comunicazioni ed adempimenti alle Autorità di Vigilanza, di archiviare e conservare la documentazione di competenza prodotta nell'ambito della gestione dei rapporti con le Autorità, ivi inclusa quella trasmessa alle Autorità anche attraverso supporto elettronico. Tale documentazione deve essere resa disponibile a richiesta delle strutture competenti e alla Struttura Pivot;
 - ogni comunicazione nei confronti delle Autorità avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Società è documentata/registrata in via informatica ed archiviata presso l'Unità Organizzativa di competenza;
 - fatte salve le situazioni in cui non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il personale che ha presenziato alla visita ispettiva assiste il Funzionario pubblico nella stesura del verbale di accertamento ed eventuale prescrizione, riservandosi le eventuali controdeduzioni, firmando, per presa visione il verbale, comprensivo degli allegati, prodotto dal Funzionario stesso;
 - ad ogni visita ispettiva da parte di Funzionari delle Autorità di Vigilanza, il Responsabile della Unità Organizzativa interessata provvede a trasmettere al Direttore Generale ed alle strutture competenti copia del verbale rilasciato dal Funzionario pubblico e degli annessi allegati. Qualora non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, i soggetti interessati dall'ispezione provvedono alla redazione di una nota di sintesi dell'accertamento effettuato e alla trasmissione della stessa al Direttore Generale e alle strutture competenti. La suddetta documentazione è archiviata dal Responsabile della Unità Organizzativa interessata dall'ispezione.

Principi di comportamento

Le Unità Organizzative a qualsiasi titolo coinvolte nel processo di gestione dei rapporti con le Autorità di Vigilanza sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati;
- l'eventuale Personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un soggetto dell'Autorità di Vigilanza di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarlo all'Organismo di

Vigilanza, secondo quanto previsto dal paragrafo 4.1 ed al Responsabile Aziendale Anticorruzione;

- devono essere puntualmente trasmesse le segnalazioni alle Autorità di Vigilanza e devono essere tempestivamente riscontrate le richieste/istanze pervenute dalle stesse Autorità;
- nell'ambito delle ispezioni effettuate da parte dei funzionari delle Autorità presso la sede della Società, fatte salve le situazioni in cui i funzionari richiedano colloqui diretti con Personale specificamente individuato, partecipano agli incontri con i funzionari stessi almeno due soggetti; laddove l'ispezione sia seguita da Strutture diverse da quella coinvolta dalla verifica è sufficiente la presenza di una sola persona della Struttura interessata, unitamente ad un'altra persona di una delle Strutture che partecipano alla verifica.

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

- ritardare senza giusto motivo o omettere l'esibizione di documenti/ la comunicazione di dati richiesti;
- ostacolare/ritardare la produzione e/o l'invio dei riscontri alle richieste/istanze pervenute dalle Autorità;
- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità di Vigilanza in errore;
- chiedere o indurre – anche a mezzo di intermediari – i rappresentanti dell'Autorità di Vigilanza a trattamenti di favore ovvero omettere informazioni dovute al fine ostacolare l'esercizio delle funzioni di Vigilanza;
- promettere o versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a rappresentanti dell'Autorità di Vigilanza a titolo personale con la finalità di promuovere o favorire interessi della Società. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione a favore di soggetti collegati, la corresponsione di incentivi in violazione della disciplina di riferimento e della normativa aziendale e, più in generale, tutte le operazioni che comportino la generazione di una perdita per la Società e la creazione di un utile per i soggetti predetti.

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

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

Premessa

Il presente protocollo si applica a tutte le unità organizzative della Società coinvolte nella gestione delle procedure acquisitive dei beni e dei servizi.

Le attività inerenti la gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali sono svolte con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere.

Tra i beni vanno considerate anche le opere dell'ingegno di carattere creativo²¹, mentre tra le prestazioni vanno ricomprese anche quelle a contenuto intellettuale di qualsiasi natura (es. legale, fiscale, tecnica, giuslavoristica, amministrativa, organizzativa, incarichi di mediazione, d'agenzia o di intermediazioni varie, ecc), ivi incluso il conferimento di incarichi professionali ovvero di consulenze.

Ai sensi del D. Lgs. 231/2001, il relativo processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di *“Corruzione contro la Pubblica Amministrazione”* nelle loro varie tipologie, *“Induzione indebita a dare o promettere utilità”*, *“Traffico di influenze illecite”*²², *“Corruzione tra privati”* e *“Istigazione alla corruzione tra privati”*.

Una gestione non trasparente del processo, infatti, potrebbe consentire la commissione di tali reati, ad esempio attraverso la creazione di fondi “neri” a seguito del pagamento di prezzi superiori all'effettivo valore del bene/servizio ottenuto.

Si intende inoltre prevenire il rischio di acquisire beni o servizi di provenienza illecita, ed in particolare il coinvolgimento in altri reati al cui rischio potrebbe essere esposta l'attività della controparte (reati contro l'industria ed il commercio; reati in materia di violazione del diritto d'autore; reati di contrabbando, reati di impiego di clandestini e di intermediazione illecita e sfruttamento del lavoro²³, ecc.).

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

L'attività di gestione delle procedure acquisitive dei beni e dei servizi si articola nei seguenti processi:

- definizione e gestione del *budget* (fatte salve esigenze/forniture occasionali);
- gestione degli approvvigionamenti;

²¹ Ai sensi dell'art. 2575 del codice civile, le opere dell'ingegno di carattere creativo tutelate dal diritto d'autore sono quelle che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì considerate e protette come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore (art. 1, L. 22 aprile 1941, n. 633).

²² Si ricorda che, ai sensi dell'art. 322 *bis* c.p., la condotta del corruttore, istigatore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, degli Enti costituiti sulla base dei Trattati che istituiscono l'UE, o, infine, nell'ambito degli altri Stati membri dell'UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

²³ Si vedano al riguardo il paragrafo 7.4 e il paragrafo 7.8.

- gestione del ciclo passivo;
- selezione e gestione dei fornitori di beni, servizi o prestazioni professionali.

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

Principi di controllo

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

- Livelli autorizzativi definiti:
 - ai sensi del sistema dei poteri e delle deleghe, il *budget* della Società è predisposto dai soggetti competenti ed approvato dal Consiglio di Amministrazione;
 - l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa applicabile illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
 - la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati in appositi albi (della Capogruppo), fatte salve esigenze/forniture occasionali. Tali fornitori devono garantire e su richiesta poter documentare anche con riferimento ai subappaltatori da loro incaricati:
 - in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi – il rispetto della disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti nonché il corretto espletamento delle pratiche doganali (ivi compreso il pagamento dei relativi diritti);
 - in relazione ai lavoratori impiegati, il rispetto della disciplina in tema di immigrazione e la regolarità retributiva, contributiva, previdenziale, assicurativa e fiscale;
 - l'eventuale affidamento a terzi – da parte dei fornitori della Società – di attività in sub-appalto, è contrattualmente subordinato ad un preventivo assenso da parte della Società;
 - l'autorizzazione al pagamento della fattura spetta al Direttore Generale o ai soggetti all'uopo incaricati; può essere negata a seguito di formale contestazione delle inadempienze/carenze della fornitura adeguatamente documentata e dettagliata;
 - il pagamento delle fatture è eseguito da una specifica funzione dedicata, a seguito di validazione di "bene eseguito" effettuato dall'Unità Organizzativa che ha usufruito del bene o del servizio.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle procedure acquisitive. In particolare, le attività di cui alle diverse fasi del processo devono essere svolte da soggetti e Unità Organizzative differenti chiaramente identificabili e devono essere supportate da un meccanismo di *maker e checker*.

- Attività di controllo:
 - la normativa interna di riferimento identifica i controlli che devono essere svolti a cura di ciascuna Unità Organizzativa interessata in ogni singola fase del processo;
 - verifica dei limiti di spesa e della pertinenza della stessa;
 - verifica della regolarità, completezza, correttezza e tempestività delle scritture contabili;
 - verifica del rispetto dei criteri individuati dal vigente sistema di deleghe e poteri e dalla normativa aziendale per la scelta dei fornitori e dei professionisti (l'avvio della relazione deve essere preceduta da un'adeguata due diligence con particolare riguardo a quanto stabilito dalle Linee Guida Anticorruzione), ivi compreso il controllo a campione del rispetto delle sopra menzionate garanzie circa l'autenticità e la legittima provenienza dei beni forniti e la regolarità dei lavoratori da loro impiegati;
 - verifica del rispetto delle norme di legge che vietano o subordinano a determinate condizioni il conferimento di incarichi di qualunque tipologia a dipendenti pubblici o ex dipendenti pubblici.

Per quanto concerne infine il conferimento di incarichi professionali e consulenze, anche qualora il suo svolgimento comporti un rapporto diretto con la Pubblica Amministrazione (quali ad esempio spese legali per contenzioso, spese per consulenze propedeutiche all'acquisizione di contributi pubblici, per verifica e deposito dei brevetti, ecc.) le Unità Organizzative interessate dovranno:

- disporre che venga regolarmente tenuto in evidenza l'elenco dei professionisti/consulenti, l'oggetto dell'incarico ed il relativo corrispettivo;
 - verificare periodicamente il suddetto elenco al fine di individuare eventuali situazioni anomale.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
 - documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi o del professionista anche attraverso gare, in termini di motivazione della scelta nonché pertinenza e congruità della spesa. La normativa interna individua in quali casi l'individuazione del fornitore di beni e/o servizi o del professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Unità Organizzativa di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi;
 - in caso di esternalizzazione di tutte o parte delle attività afferenti al processo in esame, i requisiti di tracciabilità di cui al punto precedente vengono previsti nei *Service Level Agreement* che regolano la prestazione di tali servizi e verificati periodicamente dalla Società.

Principi di comportamento

Le Unità Organizzative a qualsiasi titolo coinvolte nel processo di gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

In particolare:

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

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

- assegnare incarichi di fornitura/professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;
- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori della Società che non trovino adeguata giustificazione nel contesto del rapporto contrattuale in essere con gli stessi;
- minacciare i fornitori di ritorsioni qualora effettuino prestazioni a favore o utilizzino i servizi di concorrenti della Società;
- introdurre merci che violino prescrizioni, divieti e limitazioni di cui al Testo Unico delle disposizioni legislative in materia doganale;
- promettere versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore) e accordare

vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a favore di esponenti/rappresentanti della Pubblica Amministrazione e/o esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la Società, al fine di favorire indebitamente gli interessi della Società stessa, oppure minacciarli di un danno ingiusto per le medesime motivazioni. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini la sponsorizzazione a favore di soggetti collegati, la corresponsione di incentivi in violazione della disciplina di riferimento e della normativa aziendale oppure, più in generale, tutte le operazioni che comportino la generazione di una perdita per la Società e la creazione di un utile per i soggetti predetti.

I principi di controllo e di comportamento illustrati nel presente protocollo devono intendersi altresì estesi, per quanto compatibili, alla gestione dei rapporti con i partner scientifici, tecnologici, finanziari, etc. di cui al paragrafo 7.2.2.1 “Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione”.

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

7.2.2.7 Gestione di omaggi, spese di rappresentanza e sponsorizzazioni

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative della Società coinvolte nella gestione di omaggi, spese di rappresentanza e sponsorizzazioni.

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

- per omaggi si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine della Società;
- per spese di rappresentanza si intendono le spese sostenute dalla Società nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Società (ad es.: spese per colazioni e rinfreschi, spese per forme di accoglienza ed ospitalità, ecc.);
- per sponsorizzazioni si intendono la promozione, la valorizzazione ed il potenziamento dell'immagine della Società attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con Enti esterni (ad es.: società o gruppi sportivi che svolgono attività anche dilettantistica, Enti senza fini di lucro, Enti territoriali ed organismi locali, ecc.).

Ai sensi del D. Lgs. 231/2001, i relativi processi potrebbero costituire una delle modalità strumentali attraverso cui commettere i reati di *“Corruzione contro la Pubblica Amministrazione”*, nelle loro varie tipologie, *“Induzione indebita a dare o promettere utilità”*, *“Traffico di influenze illecite”*²⁴, *“Corruzione tra privati”* e *“Istigazione alla corruzione tra privati”*.

Una gestione non trasparente dei processi relativi agli omaggi, alle spese di rappresentanza e alle sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali e/o a persone loro subordinate di società controparti o in relazione con AFC Digital HUB, al fine di favorire interessi della Società ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo, conformi, ove applicabili e tenendo conto delle specificità organizzative e operative della Società, a quelli adottati dalla Capogruppo, risultano applicati sia a presidio delle attività svolte all'interno della Società, sia a presidio di tutte le attività esternalizzate alla Capogruppo sulla scorta del relativo contratto di servizio.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

²⁴ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore, istigatore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, degli enti costituiti sulla base dei Trattati che istituiscono l'UE, o, infine, nell'ambito degli altri Stati membri dell'UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

Descrizione del Processo

I processi di gestione degli omaggi e delle spese di rappresentanza hanno ad oggetto i beni destinati ad essere offerti, in qualità di cortesia commerciale, a soggetti terzi, quali, ad esempio, clienti e fornitori, Enti della Pubblica Amministrazione, istituzioni pubbliche o altre organizzazioni.

Si considerano atti di cortesia commerciale e/o istituzionale di modico valore gli omaggi o ogni altra utilità (ad esempio inviti ad eventi sportivi, spettacoli e intrattenimenti, biglietti omaggio, etc.) provenienti o destinati al medesimo soggetto/ente, che non superino, in un anno solare, il valore di 150 euro.

Tali beni sono acquisiti sulla base delle regole operative sancite dalla normativa interna in materia di spesa e dal protocollo “Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali” di cui al paragrafo 7.2.2.6.

I processi di gestione delle spese per sponsorizzazioni si articolano nelle seguenti fasi:

- ricezione della richiesta, inviata dagli Enti, di sponsorizzazioni per progetti, iniziative, manifestazioni;
- individuazione di società/organizzazioni cui destinare le elargizioni;
- effettuazione delle attività di *due diligence*²⁵ della Società;
- esame/valutazione dell’iniziativa/progetto proposto;
- autorizzazione alla spesa e, qualora previsto, stipula dell’accordo/ contratto;
- erogazione delle elargizioni da parte della Società.

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

Principi di controllo

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

- Livelli autorizzativi definiti:
 - per quanto attiene alle spese di rappresentanza e agli omaggi, l’approvazione delle spese sostenute per iniziative di rappresentanza, l’approvazione della richiesta di acquisto, il conferimento dell’incarico, il perfezionamento del contratto e l’emissione dell’ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno;
 - tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
 - gli omaggi o le altre utilità di valore superiore a 150 euro possono essere ammissibili in via eccezionale, in considerazione del profilo del donante o del beneficiario, e comunque nei limiti della ragionevolezza, previa autorizzazione del Presidente del Consiglio di Amministrazione o

²⁵ Ricerca di informazioni rilevanti sull’Ente richiedente quali, a titolo esemplificativo e non esaustivo denominazione, natura giuridica e data di costituzione, sede legale e operativa (se diversa da quella legale) ed eventuale sito *web*, legale rappresentante ed eventuali notizie sulla sua reputazione, notizie sull’ente e sulle sue linee strategiche, sulla dimensione (numero dipendenti e/o collaboratori, numero di soci), sui principali progetti realizzati negli ultimi due anni nel settore di riferimento dell’iniziativa proposta, sintesi delle informazioni finanziarie relative ai bilanci approvati negli ultimi due anni, ecc.

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

- sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.
- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi. In particolare, le attività di cui alle diverse fasi dei processi devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di *maker e checker*.
- Attività di controllo:
 - La normativa interna e/o di Gruppo applicabile definisce le modalità con le quali le erogazioni relative a sponsorizzazioni devono essere precedute da un'attività di *due diligence* con particolare riguardo a quanto stabilito dalle Linee Guida Anticorruzione da parte della Struttura interessata. In particolare, è prevista:
 - l'analisi e la verifica del tipo di organizzazione e della finalità per la quale è costituita;
 - la verifica ed approvazione di tutte le erogazioni da parte del Responsabile della Unità interessata;
 - la verifica che le erogazioni complessive siano stabilite annualmente e trovino capienza in apposito *budget* deliberato dagli Organi competenti;
 - è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa.

Inoltre, le Unità Organizzative interessate dovranno:

- disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero degli omaggi distribuiti nonché le relative date/occasioni delle erogazioni. Tale obbligo non si applica per gli omaggi cosiddetti "marchiati", riportanti cioè il logotipo della Società o Del Gruppo (quali biro, oggetti per scrivania, ecc.), nonché l'omaggistica *standard* (ad esempio, in occasione di fine anno);
- verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza e delle sponsorizzazioni anche attraverso la redazione, da parte di tutte le strutture interessate, di una reportistica sulle erogazioni effettuate/contratti stipulati;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Unità Organizzativa di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica,

inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza e delle sponsorizzazioni.

Principi di comportamento

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

- la Società può effettuare erogazioni sotto forma di sponsorizzazioni per sostenere iniziative di enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici della Società;
- le erogazioni devono essere riconosciute esclusivamente su un conto corrente intestato all'ente beneficiario; non è consentito effettuare pagamenti in contanti, in un Paese diverso da quello dell'ente beneficiario o a un soggetto diverso dallo stesso.

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

- effettuare erogazioni, per iniziative di sponsorizzazione, a favore di enti coinvolti in vicende giudiziarie note, pratiche non rispettose dei diritti umani, o contrarie alle norme in tema di vivisezione e di tutela dell'ambiente. Non possono essere destinatari di erogazioni partiti e movimenti politici e le loro articolazioni organizzative, organizzazioni sindacali e di patronato, club (ad esempio *Lions*, *Rotary*, ecc.), associazioni e gruppi ricreativi, scuole private, parificate e/o legalmente riconosciute, salvo specifiche iniziative connotate da particolare rilievo sociale, culturale o scientifico che devono essere approvate dal Responsabile Aziendale Anticorruzione;
- effettuare erogazioni/omaggi a favore di enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate, nonché a esponenti apicali o soggetti a loro sottoposti di società/organizzazioni di natura privatistica contravvenendo a quanto previsto nel presente protocollo e dalle Linee Guida Anticorruzione di Gruppo;
- promettere o versare/offrire - anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad esponenti apicali o soggetti a loro sottoposti di società/organizzazioni di natura privatistica con la finalità di promuovere o favorire interessi della Società, anche a seguito di illecite pressioni. Il Personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse

essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1 ed al Responsabile Aziendale Anticorruzione;

- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la Società, al fine di favorire indebitamente gli interessi della Società stessa;
- dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere nonché le indicazioni geografiche e le denominazioni di origine protette.

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

7.2.2.8 Gestione del processo di selezione e assunzione del personale

Premessa

Attualmente, anche in considerazione dell'organizzazione e operatività della Società, non è previsto l'impiego di personale dipendente.

Nel caso in cui in futuro la Società si dovesse trovare nella necessità di assumere personale dipendente, le strutture coinvolte dovranno assicurare il rispetto della normativa di Gruppo applicabile nonché delle regole definite dal presente protocollo.

Le attività inerenti l'eventuale gestione del processo di selezione e assunzione del personale prevedono il coinvolgimento/supporto delle competenti funzioni della Capogruppo per le parti e nei termini indicati nel relativo contratto di servizio stipulato con la stessa dalla Società.

Il presente protocollo si applica a tutte le Unità Organizzative della Società coinvolte nella eventuale gestione del processo di selezione e assunzione del personale.

Il processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di *“Corruzione contro la Pubblica Amministrazione”*, nelle loro varie tipologie, di *“Induzione indebita a dare o promettere utilità”*, di *“Traffico di influenze illecite”*²⁶, nonché di *“Corruzione tra privati”* e *“Istigazione alla corruzione tra privati”*.

Una gestione non trasparente del processo di selezione e assunzione del personale, potrebbe, infatti, consentire la commissione di tali reati attraverso la promessa di assunzione verso rappresentanti della Pubblica Amministrazione e/o esponenti apicali e/o persone loro subordinate di società controparti o in relazione con la Società o soggetti da questi indicati, concessa al fine di influenzarne l'indipendenza di giudizio o di assicurare un qualsivoglia vantaggio per la Società.

Sussiste altresì il rischio della commissione del reato di *“Impiego di cittadini di paesi terzi il cui soggiorno è irregolare”* che si intende presidiare anche attraverso il presente protocollo.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

L'eventuale processo di selezione e assunzione del personale si articola nelle seguenti fasi:

- selezione del personale:
 - analisi e richiesta di nuove assunzioni;
 - definizione del profilo del candidato;
 - reclutamento dei candidati;
 - svolgimento del processo selettivo;
 - individuazione dei candidati.
- Formalizzazione dell'assunzione.

²⁶ Si ricorda che, ai sensi dell'art. 322-bis c.p., la condotta del corruttore, istigatore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, degli enti costituiti sulla base dei Trattati che istituiscono l'UE, o, infine, nell'ambito degli altri Stati membri dell'UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

Le modalità operative per la gestione del processo sono disciplinate, in tutto o in parte, nell'ambito della normativa interna e/o di Gruppo applicabile, sviluppata ed aggiornata a cura delle Unità Organizzative competenti che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - accentramento del processo di selezione e assunzione del personale in capo alla funzione competente che riceve le richieste formali di nuovo personale da parte delle Unità Organizzative interessate e le valuta in coerenza con il *budget* ed i piani interni di sviluppo;
 - autorizzazione all'assunzione concessa soltanto da soggetti espressamente facoltizzati secondo il vigente sistema dei poteri e delle deleghe;
 - assunzione dei candidati individuati come idonei e per i quali è stata fornita autorizzazione all'inserimento viene effettuata dalle Unità Organizzative competenti.
- Segregazione dei compiti tra i diversi soggetti coinvolti nel processo.
- Attività di controllo:
 - compilazione da parte del candidato, al momento dello svolgimento della selezione, di un'apposita modulistica per garantire la raccolta omogenea delle informazioni sui candidati;
 - l'assunzione deve essere preceduta da un'adeguata *due diligence* con particolare riguardo a quanto stabilito dalle Linee Guida Anticorruzione di Gruppo.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, i soggetti e le strutture competenti sono responsabili dell'archiviazione e della conservazione di tutta la documentazione prodotta (tra cui quella *standard* ad esempio testi, *application form*, contratto di lavoro, ecc.) anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di selezione e assunzione del personale.

Principi di comportamento

Le Unità Organizzative a qualsiasi titolo coinvolte nell'eventuale gestione del processo di selezione e assunzione del personale, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

In particolare:

- il Personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere

destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1 ed al Responsabile Aziendale Anticorruzione;

- la selezione deve essere effettuata tra una rosa di candidati, salvo il caso di personale specialistico qualificato, di categorie protette ovvero di figure destinate a posizioni manageriali;
- la valutazione comparativa dei candidati deve essere effettuata sulla base di criteri di competenza, professionalità ed esperienza in relazione al ruolo per il quale avviene l'assunzione;
- qualora il processo di assunzione riguardi:
 - personale diversamente abile, il reclutamento dei candidati avverrà nell'ambito delle liste di soggetti appartenenti alle categorie protette, da richiedere al competente Ufficio del Lavoro;
 - lavoratori stranieri, il processo dovrà garantire il rispetto delle leggi sull'immigrazione e la verifica del possesso, per tutta la durata del rapporto di lavoro, dei permessi di soggiorno, ove prescritti;
 - ex dipendenti pubblici, il processo dovrà garantire il rispetto dei divieti di legge.
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'Unità Organizzativa/figura competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

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

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

7.2.2.9 Gestione dei rapporti con i Regolatori

Premessa

Il presente protocollo si applica a tutte le Strutture della Società coinvolte nella gestione dei rapporti con i Regolatori con potere di produzione normativa rilevante per la Società ed il Gruppo e riguarda qualsiasi tipologia di attività posta in essere in occasione di segnalazioni, adempimenti, comunicazioni, richieste, istanze. Rientrano altresì le attività di *advocacy* ovvero pareri/proposte/risposte a consultazioni su normative in corso di elaborazione o in essere. Per quanto riguarda i rapporti con le Autorità di Vigilanza, in quanto *Supervisors*, si rinvia al protocollo 7.2.2.5.

Le attività inerenti all'eventuale gestione dei rapporti con i Regolatori sono svolte con il supporto delle strutture competenti della Capogruppo,

Ai sensi del D. Lgs. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di “*Corruzione contro la Pubblica Amministrazione*” nelle loro varie tipologie, “*Induzione indebita a dare o promettere utilità*” e “*Traffico di influenze illecite*”²⁷.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti con:

- tutte le Istituzioni italiane ed estere, inclusi a mero titolo esemplificativo e non esaustivo il Parlamento Italiano e gli enti locali, il Governo, la Banca d'Italia, il Garante per la protezione dei dati personali, Governi/Parlamenti esteri, Autorità di regolamentazione in Paesi rilevanti per le attività della Società ed il Gruppo;
- tutte le Istituzioni internazionali e multilaterali, inclusi a mero titolo esemplificativo e non esaustivo le Istituzioni comunitarie (Commissione Europea, Consiglio dell'Unione Europea, Parlamento Europeo), le *European Supervisory Authorities* (“ESAs”), la Banca Centrale Europea, l'*European Data Protection Board* (“EDPB”);
- le associazioni di categoria, i “*think tank*”, i Gruppi di interesse, a cui la Società ed il Gruppo partecipa, con o senza rappresentanti permanenti, al fine di instaurare – in coerenza coi principi a tutela della concorrenza – tavoli di confronto con gli altri *player* di mercato o gli *stakeholder* della Società e del Gruppo stesso per l'elaborazione di pareri/proposte/risposte a consultazioni, su normative in corso di elaborazione o in essere.

Descrizione del Processo

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

²⁷ Si ricorda che, ai sensi dell'art. 322 *bis* c.p., la condotta del corruttore, dell'istigatore o del soggetto che cede all'induzione indebita è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguarda: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, degli Enti costituiti sulla base dei Trattati che istituiscono l'UE, o, infine, nell'ambito degli altri Stati membri dell'UE; ii) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito di altri Stati esteri o Organizzazioni pubbliche internazionali o sovranazionali, assemblee parlamentari internazionali, Corti internazionali.

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

Le “Regole di Gruppo per la gestione dei rapporti con i Supervisor e le Autorità di Regolamentazione” individuano le strutture della Banca tenute ad assicurare il coordinamento delle comunicazioni con le Autorità e la coerenza trasversale delle stesse a livello di Gruppo (c.d. Struttura Pivot).

In ragione dell'oggetto/ambito del singolo contatto o della singola tematica, la Struttura Pivot ingaggia le Strutture responsabili (c.d. Owner Funzionali”) per aspetti e contributi specifici per gli ambiti di competenza di volta in volta individuati.

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

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - i rapporti con i Regolatori sono intrattenuti dal Responsabile della Struttura di riferimento, da soggetti individuati o autorizzati in base allo specifico ruolo attribuito dal funzionigramma ovvero da soggetti individuati dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
 - gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto da soggetti incaricati.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo. In particolare le attività *advocacy* sono svolte da strutture diverse rispetto a quelle direttamente interessate dalla normativa oggetto di analisi.
- Attività di controllo:
 - controlli di completezza, correttezza ed accuratezza della documentazione trasmessa ai Regolatori da parte della Struttura interessata per le attività di competenza che devono essere supportate da meccanismi di *maker e checker*;
 - verifica del rispetto dei criteri individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti (l'avvio della relazione deve essere preceduta da un'adeguata *due diligence* con particolare riguardo a quanto stabilito dalle Linee Guida Anticorruzione).
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - le fasi principali del processo devono risultare da apposita documentazione scritta;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Struttura di volta in volta interessata è altresì responsabile dell'archiviazione e

della conservazione della documentazione di competenza anche in via telematica o elettronica, inerente alla gestione dei rapporti con i Regolatori.

Principi di comportamento

Le Strutture della Società, a qualsiasi titolo coinvolte nel processo di gestione dei rapporti con i Regolatori, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un soggetto appartenente ai Regolatori e, più in generale alla Pubblica Amministrazione, di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1. ed al Responsabile Aziendale Anticorruzione;
- il personale deve fornire ai Regolatori informazioni veritiere, corrette, accurate, aggiornate e non fallaci, avendo cura di differenziare i fatti dalle eventuali opinioni ed evitando di rappresentare le informazioni in modo tale da dare luogo, anche in via potenziale, a confusioni, fraintendimenti o errori da parte degli stessi;
- il personale deve manifestare in modo non equivoco e preliminarmente ogni conflitto di interessi – attuale o anche solo potenziale – con i Regolatori;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dei rapporti con i Regolatori e, più in generale, con la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a fornitori di servizi eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di fornitori di servizi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- chiedere o indurre – anche a mezzo di intermediari – i rappresentanti dei Regolatori e, più in generale, della Pubblica Amministrazione a trattamenti di favore;
- promettere o versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – ai rappresentanti dei Regolatori e, più in generale, ai soggetti della Pubblica Amministrazione con

la finalità di promuovere o favorire interessi della Società (ad esempio, tra i vantaggi che potrebbero essere accordati, si cita la promessa di assunzione per parenti ed affini, la sponsorizzazione a favore di soggetti collegati);

- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico, dal Codice Interno di Comportamento di Gruppo e dalle Linee Guida Anticorruzione di Gruppo; ciò al fine di prevenire il rischio di commissione di reati di corruzione nelle loro varie tipologie, di *“Induzione indebita a dare o promettere utilità”* e di *“Traffico di influenze illecite”* che potrebbe derivare dall'eventuale scelta di soggetti “vicini” a persone legate ai Regolatori e, più in generale, alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Società.

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

7.3 Area sensibile concernente i reati societari

7.3.1 Fattispecie di reato

Premessa

L'art. 25-ter del Decreto contempla quasi tutti i reati societari previsti dal Titolo XI del codice civile²⁸. I reati societari considerati hanno ad oggetto differenti ambiti, tra i quali assumono particolare rilevanza la formazione del bilancio, le comunicazioni esterne, talune operazioni sul capitale, l'impedito controllo e l'ostacolo all'esercizio delle funzioni di vigilanza, fattispecie accomunate dalla finalità di tutelare la trasparenza dei documenti contabili e della gestione societaria e la corretta informazione ai soci, ai terzi ed al mercato in generale.

Si elencano qui di seguito le fattispecie richiamate dall'art. 25-ter del Decreto.

False comunicazioni sociali (art. 2621 c.c.)

False comunicazioni sociali delle società quotate (art. 2622 c.c.)

Questi reati si realizzano tramite condotte che, con riferimento alla situazione economica, patrimoniale o finanziaria della società o del gruppo, consistono nella consapevole:

- esposizione di fatti materiali non rispondenti al vero nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico;
- omissione di fatti materiali rilevanti la cui comunicazione è imposta dalla legge.

In ogni caso, la condotta è sanzionata penalmente quando risulta rivolta a conseguire per sé o per altri un ingiusto profitto e deve essere idonea a concretamente indurre i destinatari in errore. Inoltre, l'illecito sussiste anche se si riferisce a beni posseduti o amministrati dalla società per conto terzi. Quando il falso attiene a società diverse da quelle quotate o da quelle ad esse equiparate²⁹:

- l'esposizione di fatti materiali falsi costituisce reato in questione solo se contenuta in comunicazioni sociali previste dalla legge e i fatti sono rilevanti;
- si applicano pene attenuate e la causa di esclusione della punibilità per l'ipotesi di particolare tenuità del fatto³⁰.

²⁸ L'art. 25-ter è stato modificato dalla:

- L. n. 190/2012, che ha aggiunto il riferimento al nuovo reato di "Corruzione tra privati", di cui all'art. 2635, comma 3, del codice civile, con decorrenza dal 28 novembre 2012;
- L. n. 69/2015, che ha eliminato per i reati societari i riferimenti a condizioni di responsabilità degli Enti in parte diverse da quelle ordinarie e ha riformato i reati di "False comunicazioni sociali", con decorrenza dal 14 giugno 2015.

²⁹ Alle società quotate in un mercato regolamentato nazionale o dell'Unione europea sono equiparate le società che le controllano, le società emittenti strumenti finanziari per i quali è stata chiesta l'ammissione alla negoziazione in detti mercati o che sono negoziati in un sistema multilaterale di negoziazione italiano, nonché le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

³⁰ Si veda l'art. 2621-bis del codice civile che prevede pene inferiori se i fatti sono di lieve entità, in considerazione della natura e delle dimensioni della società e delle modalità o degli effetti della condotta, oppure se i fatti riguardano le piccole società non sottoponibili a procedura fallimentare. In quest'ultimo caso il reato è procedibile solo a querela. Inoltre, l'art. 2621-ter del codice civile richiama l'applicabilità dell'art. 131-bis del codice penale che esclude la punibilità quando, per le modalità della condotta e per l'esiguità del danno o del pericolo, l'offesa è di particolare tenuità e il comportamento non risulti abituale.

Falsità nelle relazioni o nelle comunicazioni delle Società di Revisione (art. 27 D. Lgs. 39/2010)

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, circa la situazione economica, patrimoniale o finanziaria della società sottoposta a revisione, al fine di conseguire per sé o per altri un ingiusto profitto, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni.

L'illecito è più severamente sanzionato se: ha cagionato un danno patrimoniale ai destinatari delle comunicazioni; concerne la revisione di determinati enti qualificati dal predetto Decreto "di interesse pubblico" (tra cui le società quotate, gli emittenti di strumenti finanziari diffusi tra il pubblico in maniera rilevante, le banche, alcune imprese di assicurazione, le SIM, le SGR, le SICAV, gli intermediari finanziari di cui all'art. 107 T.U.B.); è commesso per denaro o altra utilità; è commesso in concorso con gli esponenti della società sottoposta a revisione.

Soggetti attivi sono in primis i responsabili della Società di Revisione (reato proprio). È altresì prevista la punibilità di chi dà o promette il denaro o l'utilità e dei direttori generali, dei componenti l'organo amministrativo e dell'organo di controllo degli enti di interesse pubblico, che abbiano concorso a commettere il fatto.

Tale fattispecie attualmente non costituisce reato presupposto della responsabilità degli enti³¹.

Impedito controllo (art. 2625 comma 2 c.c.)

Il reato di cui all'art. 2625 comma 2 del codice civile si verifica nell'ipotesi in cui gli amministratori impediscano od ostacolano, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri Organi societari, procurando un danno ai soci. Il reato è punito a querela della persona offesa e la pena è aggravata se il reato è commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante.

La fattispecie di impedito controllo nei confronti della Società di Revisione, in origine pure prevista dall'art. 2625 c.c.³², attualmente non costituisce reato presupposto della responsabilità degli enti.

³¹ L'art. 25 ter del D. Lgs. 231/2001 continua tuttora a richiamare l'art. 2624 c.c., che in origine prevedeva questo reato, nonostante l'evoluzione normativa nel frattempo intervenuta. Difatti:

- la L. n. 262/2005 introdusse l'art. 174-bis del T.U.F. che puniva con una autonoma fattispecie le falsità nella revisione delle società quotate, delle società da queste controllate e delle società che emettono strumenti finanziari diffusi fra il pubblico in misura rilevante;
- sia l'art. 2624 c.c., sia l'art. 174-bis del T.U.F. a seguito della riforma della disciplina della revisione legale dei conti, sono stati abrogati e, a decorrere dal 7.4.2010, le falsità nella revisione sono punite dalla nuova fattispecie prevista dall'art. 27 del D.Lgs. 39/2010.

Tale evoluzione ha fatto sorgere seri dubbi sulla permanente configurabilità della responsabilità degli enti per le condotte in questione. La Corte di Cassazione, con la sentenza n. 34476/2011 delle Sezioni Unite penali, ha ritenuto che il reato di falso in revisione legale quale ora previsto dall'art. 27 del D. Lgs. 39/2010 non rientri più nell'ambito di applicazione della responsabilità amministrativa degli enti, in quanto tale norma non è richiamata dall'art. 25-ter del D. Lgs. 231/2001. Va altresì considerato che determinate condotte corruttive nei confronti dei revisori dei conti sono previste e punite ai sensi degli artt. 28 e 30 del D. Lgs. 39/2010, ma non costituiscono reato presupposto della responsabilità degli enti.

³² L'art. 2625 c.c. contemplava anche il reato di impedito controllo degli amministratori nei confronti della Società di Revisione. Con la riforma della disciplina della revisione legale dei conti il reato è stato espunto dall'art. 2625 c.c. e riformulato dall'art. 29 del D. Lgs. 39/2010 e poi depenalizzato dal D. Lgs. 8/2016; poiché l'art. 25-ter del D. Lgs. 231/2001 non è stato conseguentemente modificato con l'inserimento di un richiamo anche al citato art. 29, sembra potersi affermare che l'illecito di impedito controllo nei confronti della Società di Revisione non rientri più nella disciplina della responsabilità amministrativa degli enti. Al riguardo sembra valere il medesimo principio di cui alla sentenza della Corte di Cassazione citata nella nota precedente.

Indebita restituzione dei conferimenti (art. 2626 c.c.)

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

Illegale ripartizione degli utili e 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.)

Il reato in questione si perfeziona con l'acquisto o la sottoscrizione, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della 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 altra società o scissioni, che cagionino danno ai creditori.

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

Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.)

Questo reato si perfeziona quando l'amministratore di una società con titoli quotati in un mercato regolamentato italiano o dell'Unione Europea o diffusi in misura rilevante tra il pubblico, ovvero soggetta a vigilanza ai sensi del Testo Unico Bancario, del Testo Unico dell'Intermediazione Finanziaria o delle norme disciplinanti le attività assicurative o le forme pensionistiche complementari, non comunica, nelle forme e nei termini previsti dall'art. 2391 c.c., all'organo al quale partecipa ovvero alla società e comunque al Collegio Sindacale, l'interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società in questione, ovvero se si tratta di Amministratore Delegato non si astiene dal compiere l'operazione cagionando in tal modo un danno alla società o a terzi.

Formazione fittizia del capitale (art. 2632 c.c.)

Tale reato si perfeziona nel caso in cui gli amministratori e i soci conferenti formino o aumentino 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 dei beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

Il reato si perfeziona con la ripartizione da parte dei liquidatori di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

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

Corruzione tra privati (art. 2635, commi 1 e 3, c.c.)

Istigazione alla corruzione tra privati (art. 2635-bis comma 1, c.c.)

Integra il reato di corruzione tra privati la condotta di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili, sindaci, liquidatori e degli altri soggetti investiti di funzioni direttive nell'ambito di una società o di un altro ente privato nonché dei soggetti sottoposti alla loro direzione o vigilanza che, anche per interposta persona, per sé o per altri sollecitano o ricevono denaro o altra utilità non dovuti, o ne accettano la promessa, al fine di compiere od omettere un atto contrario agli obblighi inerenti al loro ufficio o agli obblighi di fedeltà, nei confronti della società o ente privato di appartenenza .

È punito anche il corruttore, vale a dire chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuta alle predette persone.

Rispondono invece del reato di "istigazione alla corruzione tra privati" coloro che fanno una offerta o promessa che non venga accettata, o gli esponenti di società o enti privati che sollecitano la dazione o promessa, qualora la sollecitazione non sia accettata³³.

Solo le condotte del corruttore (di offerta, dazione o promesse, che siano accettate o no) e non anche quelle dei corrotti (di accettazione o di sollecitazione) costituiscono reato presupposto della responsabilità amministrativa degli enti, se commesse nell'interesse della società/ente al quale il corrotto appartiene³⁴.

Entrambi i reati sono perseguibili d'ufficio.

³³ Il reato di istigazione sussiste solo se l'offerta o la promessa sono rivolte a o la sollecitazione è formulata da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili, sindaci, liquidatori o soggetti che svolgono funzioni direttive in una società o in un ente. Non integrano l'istigazione le medesime condotte commesse da/ dirette a dipendenti che non svolgono funzioni direttive.

³⁴ La riforma del reato di corruzione tra privati e l'introduzione del reato di istigazione alla corruzione tra privati sono state disposte dal D.Lgs. 38/2017 in vigore dal 14 aprile 2017. I fatti commessi prima di tale data costituivano corruzione tra privati solo se alla condotta conseguiva effettivamente un atto contrario ai doveri e un danno per la società di appartenenza dei corrotti, e non rilevavano se colpivano enti privati diversi da società. L'inserimento anche degli enti privati parrebbe onnicomprensivo e non limitato alle sole associazioni e fondazioni dotate di personalità giuridica.

Illecita influenza sull'assemblea (art.2636 c.c.)

È punito con la reclusione chiunque determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Aggiotaggio (art. 2637 c.c.)

La fattispecie di reato si riferisce alla 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 alla negoziazione in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Per l'ipotesi di condotte riferite a emittenti strumenti quotati o per i quali sia stata chiesta l'ammissione alla negoziazione su un mercato regolamentato restano applicabili le sanzioni in materia di abusi di mercato e la connessa responsabilità amministrativa.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

Il reato in questione si realizza nel caso in cui, col fine specifico di ostacolare l'attività delle autorità pubbliche di vigilanza, si espongano in occasione di comunicazioni ad esse dovute in forza di legge, fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, ovvero si occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che si era tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi.

Il reato si perfeziona altresì mediante qualsiasi condotta attiva od omissiva che in concreto determini un ostacolo allo svolgimento delle funzioni demandate alle Autorità di Vigilanza.

La pena è aggravata se il reato è commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante.

Falso in prospetto (art. 173 bis del D. Lgs. 58/1998)

L'art. 173 bis del D. Lgs. 58/1998 punisce la condotta di chi espone false informazioni od occulta dati o notizie nei prospetti richiesti ai fini della sollecitazione al pubblico risparmio o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio.

Affinché tale condotta integri gli estremi del reato, è indispensabile che il soggetto che la pone in essere agisca con l'intenzione di ingannare i destinatari dei prospetti, al fine di conseguire un ingiusto profitto, per sé o per altri. Occorre altresì che le informazioni false od omesse siano idonee ad indurre in errore i loro destinatari.

Tale fattispecie attualmente non costituisce reato presupposto della responsabilità degli enti³⁵.

7.3.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati societari sono le seguenti:

- Gestione dei rapporti con il Sindaco Unico e con la Società di Revisione;
- Gestione dell'informativa periodica;
- Acquisto, gestione e cessione di partecipazioni e di altri asset;
- Gestione dei rapporti con le Autorità di Vigilanza.

Si riportano, per le prime tre sopraelencate attività sensibili, i protocolli che dettano i principi di controllo e di comportamento applicabili a dette attività che si completano con la normativa aziendale di dettaglio che regola le attività medesime.

Relativamente all'attività indicata all'ultimo punto, si rimanda al protocollo "Gestione dei rapporti con le Autorità di Vigilanza", avente la specifica finalità di prevenire, oltre ai reati di corruzione, nelle loro varie tipologie, anche il reato societario di cui all'art. 2638 c.c.

Con particolare riferimento alle attività sensibili ai reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*" – oltre a quelle connesse alla "Gestione dei rapporti con il Sindaco Unico e con la Società di Revisione" e all'"Acquisto, gestione e cessione di partecipazioni e di altri asset", disciplinate nell'ambito dei relativi protocolli, di cui alla presente Area sensibile – si richiamano anche le attività identificate nella "Area sensibile concernente i reati contro la Pubblica Amministrazione e il reato di corruzione tra privati" e si rimanda, pertanto, ai relativi protocolli in quanto contenenti principi che esplicano la loro efficacia preventiva anche in relazione al reato suddetto :

- "Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione";
- "Gestione dei contenziosi e degli accordi transattivi";
- "Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali";
- "Gestione di omaggi, spese di rappresentanza e sponsorizzazioni";
- "Gestione del processo di selezione e assunzione del personale".

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalla Capogruppo.

³⁵ L'art. 25-ter del D. Lgs. 231/2001 continua tuttora a richiamare l'art. 2623 c.c., che in origine prevedeva questo reato. La L. n. 262/2005 abrogò la norma e introdusse l'attuale fattispecie di falso in prospetto di cui all'art. 173-bis del D. Lgs. 58/1998. Poiché l'art. 25-ter non è stato conseguentemente modificato, sembra potersi affermare che il reato di falso in prospetto non configuri più reato presupposto ai fini della responsabilità amministrativa degli enti. Al riguardo sembra valere il medesimo principio di cui alla sentenza della Corte di Cassazione citata nella nota 29.

7.3.2.1 Gestione dei rapporti con il Sindaco Unico e con la Società di Revisione

Premessa

Il presente protocollo si applica ai membri del Consiglio di Amministrazione e a tutti gli Organi e le Unità Organizzative coinvolti nella gestione dei rapporti con il Sindaco Unico e con la Società di Revisione in occasione di verifiche e di controlli svolti in ottemperanza alle prescrizioni di legge.

Le attività inerenti la gestione dei rapporti con il Sindaco Unico con la Società di Revisione prevedono il coinvolgimento/supporto delle competenti funzioni della Capogruppo per le parti e nei termini indicati nel relativo contratto di servizio stipulato con la stessa dalla Società.

Ai sensi del D. Lgs. 231/2001, il processo in oggetto potrebbe presentare occasioni per la commissione del reato di *“Impedito controllo”*, ai sensi dell’art. 2625 del codice civile nonché dei reati di cui all’art. 27 del D. Lgs. 39/2010 (per quanto concerne la fattispecie di false relazioni o comunicazioni da parte dei responsabili della revisione, commessa in concorso con gli organi della società sottoposta a revisione) e all’art. 29 del medesimo Decreto (concernente la fattispecie di impedimento od ostacolo alle attività di revisione legale), che – nonostante il principio affermato dalla Corte di Cassazione e di cui si è dato conto nel precedente paragrafo 7.3.1. – vengono comunque tenuti in considerazione ai fini del presente protocollo.

Con riferimento alla gestione dei rapporti con il Sindaco Unico e la Società di Revisione, sussiste altresì il rischio della commissione dei reati di *“Corruzione tra privati”* e *“Istigazione alla corruzione tra privati”*, introdotti dalla L. 190/2012 tra i reati societari e descritti nel paragrafo 7.3.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti in oggetto.

Descrizione del Processo

Nell’ambito dell’attività di verifica propria del Sindaco Unico e della Società di Revisione, la gestione dei rapporti con tali soggetti si articola nelle seguenti attività:

- comunicazione delle informazioni periodiche previste;
- comunicazione di informazioni e di dati societari e messa a disposizione della documentazione, sulla base delle richieste ricevute.

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

Principi di controllo

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

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare, i rapporti con il Sindaco Unico e la Società di Revisione sono intrattenuti dai soggetti appositamente individuati ovvero dalle strutture incaricate della Capogruppo, per gli ambiti di propria competenza, in virtù dei contratti di servizio stipulati dalla Società.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con il Sindaco Unico e la Società di Revisione al fine di garantire, per tutte le fasi del processo, un meccanismo di *maker e checker*.
- Partecipazione regolare e continua del Sindaco Unico alle riunioni del Consiglio di Amministrazione, a garanzia della effettiva conoscenza da parte dell'Organo di Controllo in merito alle scelte di gestione della Società.
- Tempestiva e completa evasione, a cura delle Unità Organizzative competenti, delle richieste di documentazione specifica avanzate dal Sindaco Unico nell'espletamento della propria attività di vigilanza e controllo.
- Tempestiva e completa evasione, a cura delle Unità Organizzative competenti, delle richieste di documentazione specifica avanzate dalla Società di Revisione nell'espletamento delle proprie attività di verifica e controllo e valutazione dei processi amministrativo-contabili: ciascuna Unità Organizzativa ha la responsabilità di raccogliere e predisporre le informazioni richieste e provvedere alla consegna delle stesse, sulla base degli obblighi contrattuali presenti nel contratto di incarico di revisione, mantenendo chiara evidenza della documentazione consegnata a risposta di specifiche richieste informative formalmente avanzate dai revisori.
- Tempestiva e completa messa a disposizione della Società di Revisione, da parte delle Unità Organizzative interessate, della documentazione disponibile relativa alle attività di controllo ed ai processi operativi seguiti, sui quali i revisori effettuano le proprie attività di verifica.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - sistematica formalizzazione e verbalizzazione delle attività di verifica e controllo del Sindaco Unico;
 - verifica e conservazione delle dichiarazioni di supporto per la predisposizione delle *Representation Letter*, con firma delle dichiarazioni stesse da parte dei soggetti competenti, per l'inoltro al Dirigente Preposto della Capogruppo;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Unità Organizzativa di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla gestione dei rapporti con il Sindaco Unico e la Società di Revisione.

Principi di comportamento

Le Unità Organizzative e gli Organi a qualsiasi titolo coinvolti nella gestione dei rapporti con il Sindaco Unico e la Società di Revisione sono tenuti alla massima diligenza, professionalità, trasparenza, collaborazione, disponibilità e al pieno rispetto del ruolo istituzionale degli stessi, dando puntuale e sollecita esecuzione alle prescrizioni ed agli eventuali adempimenti richiesti nel presente protocollo, in conformità alle disposizioni di legge esistenti in materia nonché alle eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- devono essere puntualmente trasmesse le comunicazioni periodiche al Sindaco Unico e alla Società di Revisione e tempestivamente riscontrate le richieste/istanze pervenute dagli stessi;
- i membri del Consiglio di Amministrazione e i componenti delle Unità Organizzative che, a qualunque titolo, siano coinvolti in una richiesta di produzione di documenti o di informazioni da parte del Sindaco Unico o della Società di Revisione pongono in essere comportamenti improntati alla massima correttezza e trasparenza e non ostacolano in alcun modo le attività di controllo e/o di revisione;
- i dati ed i documenti devono essere resi disponibili in modo puntuale ed in un linguaggio chiaro, oggettivo ed esaustivo in modo da fornire informazioni accurate, complete, fedeli e veritiere;
- ciascuna Unità Organizzativa aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione formalmente prodotta e/o consegnata al Sindaco Unico e ai Revisori, nell'ambito della propria attività, ivi inclusa quella trasmessa in via elettronica.

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

- ritardare senza giusto motivo o omettere l'esibizione di documenti/la comunicazione di dati richiesti;
- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre il Sindaco Unico, altri organi societari e la Società di Revisione in errore di valutazione tecnico-economica della documentazione presentata;
- promettere o versare somme di denaro o altre utilità al Sindaco Unico o alla Società di Revisione con la finalità di promuovere o favorire interessi della Società.

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

7.3.2.2 Gestione dell’informativa periodica

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative coinvolte nella predisposizione dei documenti che contengono comunicazioni societarie relative alla situazione economica, patrimoniale e finanziaria della Società.

Le attività inerenti la gestione dell’informativa periodica prevedono il coinvolgimento/supporto delle competenti funzioni della Capogruppo per le parti e nei termini indicati nel relativo contratto di servizio stipulato con la stessa dalla Società.

Ai sensi del D. Lgs. 231/2001, il processo di predisposizione dei documenti in oggetto potrebbe presentare occasioni per la commissione del reato di *“False comunicazioni sociali”*, così come disciplinato agli artt. 2621, 2622 del Codice Civile - nonché i reati tributari, definiti nel paragrafo 7.10 (Area sensibile concernente i reati tributari).

Inoltre, le regole aziendali e i controlli di completezza e di veridicità previsti nel presente protocollo sono predisposti anche al fine di una più ampia azione preventiva dei reati che potrebbero conseguire a una scorretta gestione delle risorse finanziarie, quali i reati di *“Corruzione contro la Pubblica Amministrazione”*, nelle loro varie tipologie, *“Induzione indebita”*, *“Corruzione tra privati”*, *“Istigazione alla corruzione tra privati”*, nonché i reati di *“Riciclaggio”* e *“Autoriciclaggio”*.

Il processo di predisposizione dei documenti in oggetto è governato secondo linee guida declinate dal Regolamento di Intesa Sanpaolo S.p.A., approvato dall’Organo di Gestione con parere favorevole dell’Organo di Controllo, in risposta alle sollecitazioni provenienti dalla legge 28 dicembre 2005, n. 262 “Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari” ed in particolare dall’art. 154-*bis* del T.U.F., che ha qualificato normativamente la figura del “Dirigente preposto alla redazione dei documenti contabili societari” prevedendo specifiche responsabilità funzionali a garantire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria del Gruppo.

Concorrono al governo e al processo di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Società, specifici documenti di governance e regole di gruppo applicabili anche alle Società Controllate, tempo per tempo aggiornati, tra i quali si segnalano:

- le “Linee guida per il governo dell’informativa di carattere finanziario al mercato (Bilancio e Pillar III);
- le “Linee guida per la valutazione delle poste patrimoniali di bilancio”;
- le “Regole contabili di gruppo”;
- la normativa in materia di Fair Value;
- le “Regole in materia di predisposizione dell’informativa al pubblico Pillar III”.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

Nell'ambito dei processi sensibili ai fini dell'informativa finanziaria, particolare rilievo assumono le attività strettamente funzionali alla produzione del bilancio d'esercizio e delle situazioni contabili infrannuali. Tali attività attengono ai seguenti processi aziendali:

- gestione della contabilità;
- gestione del bilancio d'impresa.

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

Principi di controllo

I documenti che contengono comunicazioni societarie relative alla situazione economica, patrimoniale e finanziaria della Società devono essere redatti in base a specifiche procedure, prassi e logiche aziendali e di Gruppo che:

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

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

- Livelli autorizzativi definiti:
 - ogni Unità Organizzativa coinvolta è responsabile dei processi che contribuiscono alla produzione delle voci contabili e/o delle attività valutative ad essa demandate e degli eventuali commenti in bilancio di propria competenza;
 - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in relazione alle attività in oggetto;

- sono definiti diversi profili di utenza per l'accesso alle procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.
- Segregazione delle funzioni. Il processo di predisposizione dei documenti che contengono comunicazioni societarie relative alla situazione economica, patrimoniale e finanziaria della Società prevede il coinvolgimento di distinte Unità Organizzative, per gli ambiti di rispettiva competenza.
- Attività di controllo:
 - le attività di predisposizione dei documenti che contengono comunicazioni societarie relative alla situazione economica, patrimoniale e finanziaria della Società sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali. In particolare:
 - verifiche, con cadenza periodica, dei saldi dei conti di contabilità generale, al fine di garantirne la quadratura con i rispettivi partitari;
 - verifica, con periodicità prestabilita, di tutti i saldi dei conti lavorazione, transitori e similari, per assicurare che le Unità Organizzative interessate che hanno alimentato la contabilità eseguano le necessarie scritture nei conti appropriati;
 - esistenza di controlli *maker e checker* attraverso i quali la persona che esegue l'operazione è differente da quella che la autorizza, previo controllo di adeguatezza;
 - produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
 - analisi degli scostamenti, attraverso il confronto tra i dati contabili esposti nel periodo corrente e quelli relativi a periodi precedenti;
 - controllo di merito in sede di accensione di nuovi conti ed aggiornamento del piano dei conti;
 - quadratura della versione definitiva del bilancio con i dati contabili.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - il processo decisionale, con riferimento alle attività di predisposizione dei documenti che contengono comunicazioni societarie relative alla situazione economica, patrimoniale e finanziaria della Società è garantito dalla completa tracciabilità di ogni operazione contabile sia tramite sistema informatico sia tramite supporto cartaceo;
 - tutte le scritture di rettifica sono supportate da adeguata documentazione dalla quale è possibile desumere i criteri adottati ed, analiticamente, lo sviluppo dei relativi calcoli;
 - tutta la documentazione relativa ai controlli periodici effettuati viene archiviata presso ciascuna Unità Organizzativa coinvolta, per le voci contabili di propria competenza;
 - tutta la documentazione di supporto alla stesura del bilancio è archiviata presso l'Unità Organizzativa competente.

Principi di comportamento

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

In particolare, le Unità Organizzative sono tenute a:

- rappresentare i fatti di gestione in modo corretto, completo e tempestivo nella contabilità e nei dati aziendali allo scopo di garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari della Società;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dell'informativa periodica della Società, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto.

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

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

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

7.3.2.3 Acquisto, gestione e cessione di partecipazioni e di altri asset

Premessa

Attualmente, anche in considerazione dell'organizzazione e operatività della Società, non è previsto il compimento di attività di acquisto, gestione e cessione di partecipazioni – dirette o indirette, qualificate o non qualificate – di altre società e ad altre forme di investimento assimilabili all'assunzione di una partecipazione (quali ad esempio, la sottoscrizione di prestiti obbligazionari convertibili o di strumenti finanziari partecipativi) nonché di altri asset (ad esempio, rami d'azienda, beni e rapporti giuridici individuati in blocco).

Tuttavia, nel caso in cui in futuro la Società si dovesse trovare nella necessità di compiere le suddette attività, le strutture coinvolte dovranno coordinarsi con le strutture competenti della Capogruppo assicurare il rispetto della normativa societaria e/o di Gruppo applicabile nonché delle regole definite dal presente protocollo.

Ai sensi del D. Lgs. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di *“Corruzione tra privati”*, *“Istigazione alla corruzione tra privati”* e *“Omessa comunicazione del conflitto di interessi”*.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

Il processo si articola nelle seguenti fasi:

- esame di fattibilità dell'operazione e/o individuazione delle opportunità di investimento e/o di funding;
- gestione dei rapporti pre-contrattuali e svolgimento delle attività propedeutiche alla stipula del contratto (verifica adempimenti normativi, *due diligence*, ecc);
- perfezionamento del contratto;
- gestione degli adempimenti connessi all'acquisto, gestione e cessione di partecipazioni (compresa la designazione di esponenti presso la società partecipata) e di altri asset.

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

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:

- i soggetti che esercitano poteri autorizzativi e/o negoziali in ogni fase del processo:
 - sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal vigente sistema di poteri e deleghe ovvero dal Consiglio di Amministrazione tramite delega interna, da conservare a cura della Unità Organizzativa medesima;
 - gli atti e documenti che impegnano la Società devono essere sottoscritti da soggetti muniti dei necessari poteri;
 - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in tema di partecipazioni.
- Segregazione dei compiti tra i soggetti coinvolti nel processo al fine di garantire tra le fasi del processo un meccanismo di *maker e checker*.
- Attività di controllo:
 - verifica dell'istruttoria effettuata anche mediante l'eventuale esecuzione di specifiche attività di *due diligence* (ad es. economico/finanziaria, contabile, legale, fiscale, ecc) sull'impresa oggetto d'investimento (cd. "impresa *target*") e sulla controparte con particolare riguardo a quanto stabilito dalle Linee Guida Anticorruzione di Gruppo;
 - verifica che la delibera contenga i criteri di valutazione del prezzo dell'operazione secondo le prassi di mercato;
 - verifica del rispetto degli adempimenti legislativi e regolamentari;
 - verifica della tenuta e dell'aggiornamento dell'anagrafe delle partecipazioni in essere;
 - verifica del processo di valutazione periodica delle partecipazioni in essere nell'ambito della predisposizione della documentazione necessaria per la redazione del bilancio.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - ciascuna fase rilevante dell'attività regolata dal presente protocollo deve risultare da apposita documentazione scritta;
 - ogni accordo/convenzione/contratto/altro adempimento funzionali all'acquisto, gestione e cessione di partecipazioni e altri *asset* è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni sottostanti all'istruttoria svolta per l'assunzione della partecipazione e alle scelte effettuate nell'attività di gestione, ciascuna Unità Organizzativa coinvolta è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica oggetto del presente protocollo.

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

Principi di comportamento

Le Unità Organizzative a qualsiasi titolo coinvolte nel processo di acquisto, gestione e cessione di partecipazioni e altri asset sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo. In particolare:

- i soggetti che esercitano poteri autorizzativi e/o negoziali in sede precontrattuale, contrattuale e di gestione di rapporti partecipativi devono essere individuati e autorizzati in base allo specifico ruolo attribuito loro dal vigente sistema di poteri e deleghe ovvero dal Consiglio di Amministrazione, tramite delega interna, da conservare a cura della Unità Organizzativa medesima;
- la documentazione relativa ai contratti funzionali all'acquisto, gestione e cessione di partecipazioni e altri asset deve essere conforme alla normativa generale e speciale vigente per il settore di riferimento, anche mediante il ricorso al contributo consulenziale delle competenti Unità Organizzative e/o di professionisti esterni;
- il Personale non può dare seguito a qualunque richiesta di denaro o altra utilità di cui dovesse essere destinatario o venire a conoscenza formulata da parte di esponenti apicali, e/o persone loro subordinate di società controparti o in relazione con la Società, ivi inclusi funzionari della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1 ed al Responsabile Aziendale Anticorruzione;
- qualora sia previsto il coinvolgimento di soggetti terzi nella stipula e/o nella gestione dei contratti funzionali all'acquisto, gestione e cessione di partecipazioni e altri asset, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni coinvolti è soggetta ad un preventivo visto rilasciato dal Consiglio di Amministrazione o dalla Unità Organizzativa da questi incaricata competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;

- il Personale eventualmente designato dalla Società in qualità di componente dell'organo amministrativo di una società partecipata è tenuto a comunicare a quest'ultima – nelle forme e nei termini previsti dall'art. 2391 c.c. – l'interesse che, per conto della Società ovvero per conto proprio o di terzi, abbia in una determinata operazione della società in questione, astenendosi dall'effettuare l'operazione.

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

- comunicare dati falsi o alterati;
- promettere o versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a soggetti apicali o a soggetti sottoposti alla direzione o vigilanza dei medesimi, al fine di ottenere da parte di questi il compimento o l'omissione di un atto contrario agli obblighi inerenti il loro ufficio o agli obblighi di fedeltà con la finalità di promuovere o favorire interessi della Società. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione a favore di soggetti collegati e più in generale, tutte le operazioni che comportino la generazione di una perdita per la Società e la creazione di un utile per i soggetti predetti;
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico, dal Codice Interno di Comportamento di Gruppo e dalle Linee Guida Anticorruzione di Gruppo.

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

7.4 Area sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali, i reati contro la persona e i reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa³⁶

7.4.1 Fattispecie di reato

Premessa

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

La Capogruppo Intesa Sanpaolo ha da sempre dedicato particolare attenzione ed impegno nella collaborazione alla prevenzione di fenomeni criminali nel mercato finanziario ed al contrasto al terrorismo; un impegno che la Società assume anche ai fini della tutela della sana e prudente gestione, della trasparenza e correttezza dei comportamenti e del buon funzionamento del sistema nel suo complesso. È infatti di particolare evidenza il rischio di mettere a disposizione di clientela operante in settori inibiti dalla legge e/o appartenente o comunque contigua alla malavita organizzata servizi che risultino strumentali al perseguimento di attività illecite.

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

* * *

Sezione I – Delitti con finalità di terrorismo o di eversione dell'ordine democratico

L'art. 25-*quater* del Decreto dispone la punibilità dell'ente, ove ne sussistano i presupposti, nel caso in cui siano commessi, nell'interesse o a vantaggio dell'ente stesso, delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale, dalle leggi speciali o in violazione della Convenzione internazionale per la repressione del finanziamento del terrorismo, fatta a New York il 9.12.1999.

La norma non prevede un elenco di reati chiuso e tassativo ma si riferisce ad un qualsivoglia illecito penale caratterizzato dalla particolare finalità di terrorismo o di eversione dell'ordine democratico perseguita dal soggetto agente³⁷.

³⁶ La possibilità di commissione dei reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa, tenuto conto dell'operatività della Società, è stata ritenuta ragionevolmente remota.

³⁷ L'art. 270 *sexies* c.p. considera connotate da finalità di terrorismo le condotte che possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un organizzazione internazionale a compiere o ad astenersi dal compiere un qualsiasi atto, o di destabilizzare le strutture politiche fondamentali, costituzionali,

Con riferimento ai reati qui considerati, si può ritenere che profili di rischio rilevanti in relazione alla loro commissione possano ravvisarsi solo per i casi in cui un Organo Societario o un referente della Società agiscano in concorso con l'autore materiale del reato.

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

A) Delitti con finalità di terrorismo o eversione dell'ordine democratico previsti dal codice penale o da leggi penali speciali.

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

Le fattispecie di maggior rischio, in quanto potrebbero astrattamente presentarsi nello svolgimento dell'attività societaria, sono quelle concernenti la *"Partecipazione a prestiti a favore del nemico"* (art. 249 c.p.), il *"Sequestro di persona a scopo di terrorismo o di eversione"* (art. 289 bis c.p.) e il reato di cui all'art. 270 bis c.p., denominato *"Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico"*. In particolare, tale ultima fattispecie punisce anche qualsiasi forma di finanziamento a favore associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione.

Si richiama inoltre l'attenzione sui reati a danno del patrimonio, ed in particolare sulle fattispecie di riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, beninteso qualora commessi strumentalmente al perseguimento di finalità di terrorismo o eversione dell'ordine democratico.

Accanto alle disposizioni del codice penale, vengono in considerazione i reati previsti in leggi speciali attinenti alle più varie materie (ad. Es. in materia di armi, di stupefacenti, di tutela ambientale, ecc.) nonché in tutta quella parte della legislazione italiana, emanata negli anni '70 e '80, volta a combattere il terrorismo (ad es. in tema di sicurezza della navigazione aerea e marittima, ecc.).

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

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

* * *

economiche e sociali, nonché le altre condotte previste da convenzioni o da norme internazionali. Secondo la giurisprudenza (Cassazione. penale. n. 39504/2008) l'espressione "eversione dell'ordine democratico" non può essere limitata al solo concetto di azione politica violenta, ma deve intendersi riferita all'ordinamento costituzionale, e quindi ad ogni mezzo di lotta politica che tenda al sovvertimento del sistema democratico e costituzionale esistente o alla deviazione dai principi fondamentali che lo governano.

Sezione II – Delitti di criminalità organizzata

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

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

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

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

La norma si applica anche alla camorra e alle altre associazioni, comunque denominate, anche straniere, che presentino i connotati mafiosi predetti. Lo scambio elettorale politico-mafioso invece è commesso da chi accetta la promessa e da chi promette di procurare voti mediante le modalità di

cui al terzo comma dell'articolo 416-*bis* c.p. (i.e. le modalità proprie dell'associazione mafiosa) in cambio dell'erogazione o della promessa di erogazione di denaro o di altra utilità.

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

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

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

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

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

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

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

Si tratta di fattispecie previste dalle leggi speciali vigenti in materia (in particolare dalla L. n. 110/1975 e dalla L. 895/1967), che puniscono le condotte di illegale fabbricazione, introduzione nello Stato,

vendita, cessione, detenzione e porto abusivo di esplosivi, di armi da guerra e di armi comuni da sparo, con esclusione di quelle da bersaglio da sala, o ad emissione di gas, o ad aria compressa. Per completezza, si fa presente che la Legge 220/2021 “Misure per contrastare il finanziamento delle imprese produttrici di mine antipersona, di munizioni e submunizioni a grappolo” ha espressamente previsto il divieto del finanziamento di società aventi sede in Italia o all'estero, che, direttamente o tramite società controllate o collegate svolgano attività di costruzione, produzione, sviluppo, assemblaggio, riparazione, conservazione, impiego, utilizzo, immagazzinaggio, stoccaggio, detenzione, promozione, vendita, distribuzione, importazione, esportazione, trasferimento o trasporto delle mine antipersona, delle munizioni e submunizioni cluster, di qualunque natura o composizione, o di parti di esse. La Legge vieta altresì di svolgere ricerca tecnologica, fabbricazione, vendita e cessione, a qualsiasi titolo, esportazione, importazione e detenzione di munizioni e submunizioni cluster, di qualunque natura o composizione, o di parti di esse.

La Legge prevede in particolare che gli intermediari abilitati³⁸ che non osservino detto divieto sono puniti con la sanzione amministrativa pecuniaria da euro 150.000 a euro 1.500.000, per i casi di cui all'articolo 5 del decreto legislativo 8 giugno 2001, n. 231 (ovvero per le violazioni commesse nel loro interesse o vantaggio)³⁹.

* * *

Sezione III – Delitti transnazionali

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

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

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

³⁸ Società di intermediazione mobiliare (SIM) italiane, le banche italiane, le società di gestione del risparmio (SGR) italiane, le società di investimento a capitale variabile (SICAV), gli intermediari finanziari iscritti nell'elenco di cui all'articolo 106 del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, ivi inclusi i confidi, le banche di Paesi membri dell'Unione europea, le imprese di investimento di Paesi membri dell'Unione europea, le banche extracomunitarie, gli agenti di cambio iscritti nel ruolo unico nazionale tenuto dal Ministero dell'economia e delle finanze, nonché le fondazioni di origine bancaria e i fondi pensione

³⁹ In coerenza con i valori e i principi espressi nel Codice Etico, Intesa Sanpaolo S.p.A. vieta di porre in essere ogni tipo di attività bancaria e/o di finanziamento connessa con la produzione e/o la commercializzazione di armi controverse e/o bandite da trattati internazionali, quali: (i) armi nucleari, biologiche e chimiche; (ii) bombe a grappolo e a frammentazione; (iii) armi contenenti uranio impoverito; (iv) mine terrestri anti-persona.

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

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

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

Reati in tema di immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5 del D. Lgs. 286/1998)⁴⁰

La norma punisce le condotte consistenti nel trasportare illegalmente stranieri nel territorio dello Stato, nel promuovere, dirigere, organizzare o finanziare tale trasporto, oppure in altri atti diretti a procurare illegalmente l'ingresso di stranieri nel territorio italiano o di uno Stato diverso da quello di loro appartenenza o residenza permanente. È però richiesto che ricorra almeno una delle cinque condizioni elencate dalla norma stessa⁴¹.

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

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

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

Il reato è commesso da chi, con violenza o minaccia o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci coloro che siano

⁴⁰ I reati in tema di immigrazioni clandestine, anche se privi delle caratteristiche della transnazionalità, comportano la responsabilità ai sensi del D. Lgs. 231/2001, a decorrere dal 19 novembre 2017, data di entrata in vigore dell'art. 25 *duodecies*, comma 1 *bis*, del Decreto, introdotto dalla L. 161/2017.

⁴¹ In sintesi: a) procurato ingresso o permanenza illegale di cinque o più persone; b) pericolo per l'incolumità delle persone trasportate; c) loro trattamento degradante; d) fatti commessi da tre o più persone concorrenti o con utilizzo di servizi di trasporto internazionali o di documenti falsi o illegalmente ottenuti; e) fatti commessi da chi è nella disponibilità di armi o di esplosivi.

chiamati a rendere dichiarazioni davanti all’Autorità Giudiziaria, utilizzabili in un procedimento penale, ed abbiano la facoltà di non rispondere.

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

Favoreggiamento personale (art. 378 c.p.)

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

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

* * *

Sezione IV – Delitti contro la persona

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

In particolare, sono contemplate le fattispecie delittuose qui di seguito elencate: “*Riduzione o mantenimento in schiavitù o in servitù*” (art. 600 c.p.), “*Prostituzione minorile*” (art. 600-*bis* c.p.), “*Pornografia minorile*” (art. 600-*ter* c.p.), “*Detenzione o accesso a materiale pornografico minorile*” (art. 600-*quater* c.p.), “*Pornografia virtuale*” (art.600-*quater*.1 c.p.), “*Iniziativa turistiche volte allo sfruttamento della prostituzione minorile*” (art. 600-*quinquies* c.p.), “*Tratta di persone*” (art. 601 c.p.), “*Acquisto e alienazione e di schiavi*” (art. 602 c.p.), “*Adescamento di minorenni*” (art. 609-*undecies* c.p.).

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

Il rischio di responsabilità per i delitti in questione si può ritenere rilevante solo con riferimento all’ipotesi in cui un esponente o un referente della Società agiscano in concorso con l’autore materiale del reato.

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

- “*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*” (art. 22, comma 12-*bis*, del D. Lgs. 286/1998 – Testo Unico sull’immigrazione richiamato dall’art. 25-*duodecies* del Decreto⁴²), che punisce i datori di lavoro che assumano o si avvalgano di dipendenti extracomunitari privi di permesso di soggiorno, ovvero scaduto senza che sia richiesto il rinnovo, revocato, o annullato. La responsabilità dell’ente è prevista solo al ricorrere di determinate circostanze aggravanti⁴³;
- “*Intermediazione illecita e sfruttamento del lavoro*” (art. 603 *bis* c.p., richiamato dall’art. 25-*quinqüies* del Decreto⁴⁴), che punisce chi, approfittando dello stato di bisogno dei lavoratori, intermedia, utilizza, assume o impiega manodopera in condizioni di sfruttamento. Tra gli indici di sfruttamento sono considerate situazioni quali la corresponsione di retribuzioni difformi dai contratti collettivi, la reiterata violazione della normativa sull’orario di lavoro e i riposi, la violazione delle norme sulla sicurezza e igiene dei luoghi di lavoro;
- “*Razzismo e xenofobia*” (art. 604-*bis*, comma 3, c.p., richiamato dall’art. 25-*terdecies* del Decreto), che punisce l’incitazione, l’istigazione o la propaganda della discriminazione o della violenza per motivi razziali, etnici, nazionali o religiosi, che si basino sulla negazione o minimizzazione della Shoah o di altri crimini di genocidio, di guerra o contro l’umanità.

* * *

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

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

La possibilità di commissione dei reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa, tenuto conto dell’operatività della Società, si ritiene ragionevolmente remota.

7.4.2 Attività aziendali sensibili

Il rischio che siano posti in essere i reati con finalità di terrorismo o di eversione dell’ordine democratico, i reati di criminalità organizzata e i reati transnazionali riguarda principalmente,

⁴² L’art. 25 *duodecies* è stato inserito nel D. Lgs. 231/2001 dall’art. 2 del D. Lgs. 109/2012, in vigore dal 9.8.2012.

⁴³ Deve sussistere una delle seguenti circostanze: a) impiego di più di tre lavoratori irregolari; b) impiego di lavoratori irregolari minori in età non lavorativa; c) esposizione a situazioni di grave pericolo.

⁴⁴ Il richiamo dell’art. 603 *bis* è stato aggiunto all’art. 25 *quinqüies* del Decreto dall’art. 6 della L.199/2016, in vigore dal 4.11.2016.

nell'ambito dell'attività della Società, la gestione dei rapporti con le controparti, in particolare partner scientifici, tecnologici, finanziari, etc.

Ai fini della prevenzione dei reati in questione, l'attività si deve basare sul fondamentale principio dell'adeguata conoscenza della controparte.

Inoltre, per quanto concerne il reato di:

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

Invece, come precedentemente evidenziato, stante l'attuale operatività della Società, si ritiene ragionevolmente remota la possibilità di commissione dei reati in materia di:

- frodi sportive e di esercizio abusivo di gioco o di scommessa.

Si rimanda pertanto ai seguenti protocolli, i quali contengono principi di controllo e principi di comportamento atti a prevenire anche la commissione dei reati di cui alla presente area sensibile:

- Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione;
- Gestione dei contenziosi e degli accordi transattivi;
- Gestione del processo di selezione e assunzione del personale;
- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali.

Tenuto conto, altresì, che le attività sensibili in oggetto potrebbero presentare occasioni per la commissione dei reati di “ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio” si rimanda al protocollo:

- *“Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose”*, il quale contiene principi di controllo e principi di comportamento atti a prevenire anche la commissione dei reati di cui alla presente area sensibile.

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalla Capogruppo e/o *outsourcer* esterni.

7.5 Area sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio

7.5.1 Fattispecie di reato

Premessa

L'art. 25-*octies* del D. Lgs. 231/2001, introdotto dal D. Lgs. n. 231/2007 ("Decreto antiriciclaggio"), ha esteso la responsabilità dell'Ente ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita anche per le ipotesi in cui non siano commessi con finalità di terrorismo o di eversione dell'ordine democratico (cfr. "Area sensibile concernente i reati con finalità di terrorismo o di eversione dell'ordine democratico) o non presentino le caratteristiche di transnazionalità in precedenza previste⁴⁵. Successivamente, l'art. 25-*octies* è stato modificato aggiungendovi il reato di autoriciclaggio⁴⁶.

Da ultimo, il Decreto 195/2021 di attuazione della direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale ha previsto l'ampliamento delle condotte illecite riconducibili ai reati presupposto di ricettazione, riciclaggio, impiego di denaro, beni e utilità di provenienza illecita e autoriciclaggio che ora, in particolare, ricomprendono anche: i) i delitti colposi e ii) i reati "contravvenzionali", quest'ultimi a condizione che siano punibili con l'arresto superiore nel massimo a 1 anno o nel minimo a 6 mesi.

La riforma dei reati comporta un ampliamento delle ipotesi in cui l'ente potrà essere ritenuto responsabile, dal momento che aumentano le condotte riconducibili alla commissione dei reati presupposto di cui all'art. 25 *octies*, ad esempio, un ambito in cui possono valutarsi ampliati i rischi per l'ente è quello della salute e sicurezza nei luoghi di lavoro (D. Lgs. 81/2008).

Il rafforzamento della disciplina della responsabilità amministrativa degli enti intende prevenire e reprimere più efficacemente il fenomeno dell'immissione nel circuito economico lecito di denaro, beni od utilità provenienti dalla commissione di delitti, in quanto di ostacolo all'amministrazione della giustizia nelle attività di accertamento dei reati e di persecuzione dei colpevoli, oltre che, più in generale, lesiva dell'ordine economico, dell'integrità dei mercati e della libera concorrenza, in ragione degli indebiti vantaggi competitivi di cui godono gli operatori che dispongono di capitali di origine illecita.

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

⁴⁵ Si ricorda che ai sensi dei commi 5 e 6 dell'art. 10 L. 146/2006, abrogati dal Decreto antiriciclaggio, il riciclaggio e l'impiego illecito costituivano reati presupposto della responsabilità degli Enti solo se ricorrevano le caratteristiche di transnazionalità previste dall'art. 3 della medesima legge.

⁴⁶ Il reato di autoriciclaggio è stato inserito nel codice penale e aggiunto ai reati presupposto del D. Lgs. 231/2001 dalla Legge n. 186/2014, entrata in vigore il 1.1.2015

Ricettazione (art. 648 c.p.)

Commette il reato di ricettazione chiunque, allo scopo di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi reato, alla cui commissione non ha partecipato, o comunque si intromette nel farli acquistare, ricevere od occultare. Per tale reato è richiesta la presenza di dolo specifico da parte di chi agisce, e cioè la coscienza e la volontà di trarre profitto, per sé stessi o per altri, dall'acquisto, ricezione od occultamento di beni provenienti da reato.

E' inoltre richiesta la conoscenza della provenienza da reato del denaro o del bene; la sussistenza di tale elemento psicologico potrebbe essere riconosciuta in presenza di circostanze gravi ed univoche – quali ad esempio la qualità e le caratteristiche del bene, le condizioni economiche e contrattuali inusuali dell'operazione, la condizione o la professione del possessore dei beni – da cui possa desumersi che nel soggetto che ha agito poteva formarsi la certezza della provenienza illecita del denaro o del bene.

Riciclaggio (art. 648-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui il soggetto agente, che non abbia concorso alla commissione del delitto sottostante, sostituisca o trasferisca denaro, beni od altre utilità provenienti da un reato, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

La norma va interpretata come volta a punire coloro che – consapevoli della provenienza da reato di denaro, beni o altre utilità – compiano le operazioni descritte, in maniera tale da creare in concreto difficoltà alla scoperta dell'origine illecita dei beni considerati.

Non è richiesto, ai fini del perfezionamento del reato, l'aver agito per conseguire un profitto o con lo scopo di favorire gli autori del reato sottostante ad assicurarsene il provento. Costituiscono riciclaggio le condotte dinamiche, atte a mettere in circolazione il bene, mentre la mera ricezione od occultamento potrebbero integrare il reato di ricettazione. Come per il reato di ricettazione, la consapevolezza dell'agente in ordine alla provenienza illecita può essere desunta da qualsiasi circostanza oggettiva grave ed univoca.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)

La condotta criminosa si realizza attraverso l'impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da reato, fuori dei casi di concorso nel reato d'origine e dei casi previsti dagli articoli 648 (ricettazione) e 648-bis (riciclaggio) c.p. Rispetto al reato di riciclaggio, pur essendo richiesto il medesimo elemento soggettivo della conoscenza della provenienza illecita dei beni, l'art. 648 *ter* circoscrive la condotta all'impiego di tali risorse in attività economiche o finanziarie. Peraltro, in considerazione dell'ampiezza della formulazione della fattispecie del reato

di riciclaggio, risulta difficile immaginare condotte di impiego di beni di provenienza illecita che già non integrino di per sé il reato di cui all'art. 648 *bis* c.p.

Autoriciclaggio (art. 648-ter.1 c.p.)

Risponde del reato di autoriciclaggio chi, avendo commesso o concorso a commettere un qualsiasi reato dal quale provengono denaro, beni, o altre utilità, su tali proventi compie operazioni di impiego, sostituzione o trasferimento in attività economiche, finanziarie, imprenditoriali o speculative, con modalità tali da ostacolare concretamente l'identificazione della loro provenienza da reato.

È esclusa la punibilità delle condotte consistenti nella destinazione dei proventi illeciti alla mera utilizzazione o godimento personale. È prevista un'aggravante di pena se il fatto è commesso nell'esercizio di attività professionale, bancaria o finanziaria e un'attenuante per il caso di ravvedimento operoso del reo.

Considerazioni comuni ai reati.

Oggetto materiale.

L'oggetto materiale dei reati può essere costituito da qualsiasi entità economicamente apprezzabile e possibile oggetto di scambio, quale il denaro, i titoli di credito, i mezzi di pagamento, i diritti di credito, i preziosi, i beni materiali ed immateriali in genere.

Deve però trattarsi di bene o utilità proveniente da reato (non vengono dunque in considerazione le contravvenzioni: risulta pertanto escluso, ad esempio, il prodotto o il profitto del reato contravvenzionale di false comunicazioni sociali di cui all'art. 2621 c.c.), vale a dire esso ne deve costituire il prodotto (risultato, frutto ottenuto dal colpevole con la commissione del reato), il profitto (lucro o vantaggio economico ricavato dal reato) o il prezzo (compenso dato per indurre, istigare, determinare taluno alla commissione del reato).

Oltre che i delitti tipicamente orientati alla creazione di capitali illeciti (ad es.: concussione, corruzione, appropriazione indebita, truffa, reati fallimentari, traffico di armi o di stupefacenti, usura, frodi comunitarie, ecc.), anche i reati in materia fiscale potrebbero generare proventi oggetto di riciclaggio o di autoriciclaggio, non solo nel caso di frodi (ad es. utilizzo di fatture per operazioni inesistenti che determinino un fittizio credito Iva da detrarre), ma anche nel caso in cui l'utilità economica conseguente al reato consista in un mero risparmio di imposta per mancato esborso di denaro proveniente da attività lecite (ad es., omessa o infedele dichiarazione di redditi, per importi oltre le soglie di rilevanza penale). Anche i numerosi reati contravvenzionali⁴⁷ previsti dal nostro

⁴⁷ Inclusi, come detto nelle premesse, tra le condotte che possono costituire il presupposto per la commissione dei reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio.

Ordinamento (ad. Es. nel codice penale, nel TUB, nel TUF, nelle normative su igiene e sicurezza sul lavoro e su ambiente e rifiuti) potrebbero costituire l'antefatto per la commissione di detti reati.

Condotta ed elemento soggettivo.

Risponde dei reati di ricettazione, riciclaggio o reimpiego illecito, a seconda dei casi, il terzo estraneo al reato che genera i proventi illeciti e che li riceve dal reo (o da altri, comunque conoscendone la provenienza illecita), per compiere su di essi le condotte previste dai reati medesimi.

Potrebbe invece rispondere a titolo di concorso nel reato d'origine dei proventi illeciti e, di conseguenza, anche nel successivo reato di autoriciclaggio, qualora ne realizzi la condotta, il soggetto che avesse fornito un contributo causale di qualsiasi tipo, morale o materiale, alla commissione del reato d'origine, ad es. determinando o rafforzando il proposito criminoso del reo con la promessa, ancor prima della commissione del reato, del suo aiuto nel riciclare/impiegare i proventi.

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

Circa l'elemento soggettivo, come già accennato, i reati in esame devono essere caratterizzati dalla consapevolezza della provenienza da reato del bene. Secondo un'interpretazione particolarmente rigorosa, sarebbe sufficiente anche l'aver agito nel dubbio della provenienza illecita, accettandone il rischio (cosiddetto dolo indiretto od eventuale).

Correlazioni col reato d'origine dei proventi illeciti.

I reati della presente Area sensibile sussistono nelle ipotesi in cui le relative condotte siano successive al perfezionamento del reato che ha dato origine ai proventi illeciti, anche se compiute dopo la sua estinzione (ad es. per prescrizione o morte del reo), o anche se l'autore del medesimo non sia imputabile o punibile, oppure manchi una condizione di procedibilità (ad es., per difetto di querela, oppure di richiesta del Ministro della Giustizia, necessaria per perseguire i reati comuni commessi all'estero, ai sensi degli artt. 9 e 10 c.p.).⁴⁸

⁴⁸ In ordine all'irrelevanza dell'estinzione del reato che costituisce presupposto di un altro reato si veda l'art. 170, comma 1, c.p.; per l'irrelevanza del difetto di una condizione di punibilità o procedibilità si veda l'art. 648, comma 3, c.p., richiamato anche dagli artt. 648-bis, 648-ter e 648-ter.1 c.p.

7.5.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati di cui alla presente area sensibile, tenuto conto della specifica operatività della Società, sono quelle connesse alla gestione dei rapporti con le controparti, in particolare partner scientifici, tecnologici, finanziari, etc.

L'attività di prevenzione si basa sull'approfondita conoscenza delle controparti e sull'osservanza degli adempimenti previsti dalla normativa in tema di contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo.

Il rischio assume connotati diversi e appare meno rilevante laddove la Società compie operazioni strumentali, acquista partecipazioni o movimentata il proprio patrimonio, assolve gli adempimenti contabili e fiscali o previsti dalle specifiche normative di settore. In tali ambiti difatti, sussiste una sviluppata articolazione dei presidi di controllo e delle procedure, già imposti dalla normativa di settore (ad esempio D. Lgs. 81/2008, D. Lgs. 152/2006, etc.), al fine di assicurare il rispetto di principi di trasparenza, correttezza, oggettività e tracciabilità della gestione.

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose. Si evidenzia altresì che nell'ambito di protocolli che regolano altre attività sensibili – quali la “Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione”, la “Gestione dei contenziosi e degli accordi transattivi”, la “Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali” e la “Gestione di omaggi, spese di rappresentanza e sponsorizzazioni” – sono previsti alcuni principi di controllo e di comportamento ispirati al medesimo criterio dell'attenta valutazione di fornitori, consulenti, *partner* e controparti contrattuali in genere, principi che esplicano la loro efficacia preventiva anche in relazione ai reati sopra illustrati.

Più in generale, tutti i protocolli del presente Modello, laddove tesi a prevenire la commissione di reati che possono generare proventi illeciti, si devono intendere predisposti anche al fine della prevenzione dei reati di riciclaggio in senso lato.

Detti protocolli si applicano anche a presidio delle attività svolte, sulla base di appositi contratti di servizio, dalla Capogruppo e/o *outsourcer* esterni.

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

Premessa

Il presente protocollo si applica a tutte le strutture, anche della Capogruppo che operano per conto della Società in base al contratto di servizio in essere, coinvolte, per quanto rileva ai fini del contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose, nell'attività sensibile sopra richiamate.

Il presente Protocollo ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi di controllo e di comportamento per il contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose anche in considerazione delle vigenti disposizioni aziendali e, in particolare, la normativa interna in materia tempo per tempo vigente ove applicabile.

Descrizione del Processo

Ai fini del contrasto al finanziamento del terrorismo e al riciclaggio dei proventi di attività criminose, l'ambito di operatività rilevante per la Società riguarda l'identificazione e la conoscenza dei soggetti con cui intende instaurare rapporti contrattuali (es. *partner*, fornitori, etc.).

Rispetto a tali soggetti deve essere valutato il profilo di rischio e cioè la probabilità di esposizione ai fenomeni di riciclaggio o di finanziamento del terrorismo. La valutazione della sussistenza di tale rischio si basa sulla stessa conoscenza delle controparti e tiene conto, in particolare, di aspetti oggettivi (attività svolte dalle controparti, operazioni da essi compiute e strumenti utilizzati⁴⁹) e di aspetti soggettivi (soggetti sottoposti ad obblighi rafforzati di adeguata verifica, soggetti collegati con Paesi che presentano carenze nei presidi di prevenzione del riciclaggio o criticità sotto il profilo della cooperazione in ambito fiscale, ecc).

Particolare attenzione deve essere posta nel rilevare il possibile coinvolgimento in operazioni o rapporti con soggetti (persone fisiche e giuridiche) censiti in liste pubbliche emanate in ambito nazionale e internazionale ("Black List" ONU, UE, OFAC, ecc.).

È necessaria, inoltre, la valutazione dell'operatività disposta dalla controparte riguardante soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione – ad esempio embargo sulle armi).

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

⁴⁹ Ad esempio interposizione di soggetti terzi, impiego di strumenti societari, associativi o fiduciari suscettibili di limitare la trasparenza della proprietà e della gestione; utilizzo di denaro contante o di strumenti al portatore.

Principi di controllo

Il sistema di controllo a presidio del processo sopra descritto si basa sui seguenti fattori:

- Livelli autorizzativi e responsabilità definite:
 - la normativa interna e di Gruppo individua i soggetti e le Strutture responsabili dell'attivazione/gestione/controllo dei processi sopra descritti.
- Segregazione dei compiti:
 - i soggetti a cui competono le attività di controllo per un'adeguata conoscenza delle controparti sono differenti rispetto ai soggetti che sottoscrivono gli atti che impegnano contrattualmente la Società con le stesse.
- Attività di controllo:
 - Svolgimento, secondo un approccio risk based, all'atto dell'accensione del rapporto, di un'attività di due diligence sulla controparte da parte dell'Unità Organizzativa deputata e con il supporto delle strutture della Capogruppo competenti, finalizzato a valutare eventuali profili di rischio e la (potenziale) esposizione a fenomeni di riciclaggio o di finanziamento del terrorismo.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, i soggetti e le strutture di volta in volta interessate sono responsabili dell'archiviazione e della conservazione della documentazione di competenza raccolta e prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto.

Principi di comportamento

Le strutture della Società, a qualsiasi titolo coinvolte nelle attività sensibili individuate nell'ambito del presente Protocollo sono tenute a osservare i principi illustrati nello stesso, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo e delle Linee Guida Anticorruzione di Gruppo.

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

- instaurare rapporti contrattuali con soggetti relativamente ai quali si sospetta vi sia una relazione con il riciclaggio e/o con il finanziamento del terrorismo;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio, con il finanziamento del terrorismo;

- ricevere o occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;
- sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
- partecipare a uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione;
- mettere a disposizione di soggetti appartenenti o comunque contigui alla malavita organizzata servizi o risorse finanziarie che risultino strumentali al perseguimento di attività illecite.

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

7.6 Area sensibile concernente i reati in tema di salute e sicurezza sul lavoro

7.6.1 Fattispecie di reato

Premessa

L'art. 25-*septies* del Decreto prevede tra gli illeciti presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Il c.d. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro (D. Lgs. 9 aprile 2008 n. 81) che ha profondamente riordinato le molteplici fonti normative previgenti in materia, ha previsto all'art. 30 le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.

Finalità delle citate disposizioni è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione alla recrudescenza del fenomeno degli incidenti sul lavoro ed alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.

Si fornisce qui di seguito una sintetica descrizione dei reati sopra menzionati.

Omicidio colposo (art. 589 c.p.)

Lesioni personali colpose gravi o gravissime (art. 590 comma 3 c.p.)

Le condotte punite dalle due fattispecie consistono nel cagionare per colpa, rispettivamente, la morte oppure una lesione dalla quale deriva una malattia, nel corpo o nella mente, grave o gravissima.

Per lesioni gravi si intendono quelle che causano una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

Ai sensi del predetto art. 25-*septies* del Decreto, entrambe le condotte devono essere caratterizzate dalla violazione delle norme dettate ai fini della prevenzione degli infortuni sul lavoro e sulla tutela dell'igiene e della salute sul lavoro.

Vengono a tal proposito in considerazione molteplici disposizioni, ora in gran parte confluite nel Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro a seguito dell'abrogazione da parte del medesimo Testo Unico di varie leggi speciali previgenti, tra le quali, fondamentalmente: il D.P.R. 27.4.1955 n. 547 in tema di prevenzione degli infortuni; il D.P.R. 19.3.1956 n. 303 che disciplinava l'igiene del lavoro; il D. Lgs. 19.9.1994 n. 626 che conteneva norme generali sulla tutela della salute e della sicurezza dei lavoratori; il D. Lgs. 14.8.1996 n. 494

in tema di sicurezza dei cantieri. A completamento del corpo normativo delineato dalle specifiche misure di prevenzione prescritte dalle leggi in materia si colloca la più generale previsione di cui all'art. 2087 del codice civile, in forza della quale il datore di lavoro deve adottare le misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie per tutelare l'integrità fisica e morale dei lavoratori.

Va infine tenuto presente che la giurisprudenza ritiene che i reati in questione siano imputabili al datore di lavoro anche qualora la persona offesa non sia un lavoratore, ma un estraneo, purché la sua presenza sul luogo di lavoro al momento dell'infortunio non abbia caratteri di anormalità ed eccezionalità.

7.6.2 Attività aziendali sensibili

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

Di seguito si riporta il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di salute e sicurezza sul lavoro. Tale protocollo si completa con la normativa aziendale di dettaglio vigente in argomento.

Detto protocollo si applica anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, dalla Capogruppo e/o *outsourcer* esterni.

7.6.2.1 Gestione dei rischi in materia di salute e sicurezza sul lavoro

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative coinvolte nella gestione dei rischi in materia di salute e sicurezza sul lavoro che riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D. Lgs. 81/2008 (di seguito Testo Unico).

Si rammenta anzitutto che, ai sensi del Testo Unico compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e compete al Committente e/o ai suoi delegati la responsabilità e la gestione dei cantieri temporanei o mobili disciplinati dal Titolo IV del Testo Unico nonché compete ad entrambi, per gli ambiti di propria pertinenza, il rispetto degli obblighi relativi all'affidamento di contratti d'appalto, d'opera o di somministrazione previsti dall'art. 26 del medesimo Testo Unico.

Le attività inerenti alla gestione dei rischi in materia di salute e sicurezza sul lavoro prevedono il coinvolgimento/supporto delle competenti funzioni della Capogruppo per le parti e nei termini indicati nel relativo contratto di servizio stipulato con la stessa dalla Società.

In ottemperanza a quanto disposto dalla predetta normativa, la Società adotta e tiene aggiornato il "Documento di Valutazione dei Rischi", che contiene:

- la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;
- l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori ed il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione, dei Rappresentanti dei Lavoratori per la Sicurezza e dei Medici Competenti che hanno partecipato alla valutazione del rischio;
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Tale Documento è redatto in conformità alla normativa nazionale ed alle linee guida nazionali ed Europee (ISPESL, INAIL, UNI-EN-ISO, Agenzia Europea per la Salute e Sicurezza). In particolare, sono recepite le "Linee Guida per un Sistema di Gestione della Salute e Sicurezza sul Lavoro (SGSL)" UNI – INAIL del settembre 2001. A tal fine il Documento di Valutazione del Rischio individua, all'interno dell'organizzazione aziendale, le responsabilità, le procedure, i processi e le

risorse per la realizzazione della propria politica di prevenzione nel rispetto delle norme di salute e sicurezza vigenti. Nel medesimo Documento vengono descritte le modalità con le quali l'organizzazione risponde ai requisiti delle predette Linee Guida e sono esplicitati i processi operativi ed i documenti societari atti a garantire l'adempimento di quanto previsto dall'art. 30 – Modelli di organizzazione e di gestione – del Testo Unico.

Il “Sistema di Gestione Aziendale della Salute e Sicurezza nei Luoghi di Lavoro” è conforme alle leggi vigenti e prende come riferimento il più avanzato *standard* in materia: UNI ISO 45001 (nel 2018 lo *Standard* Internazionale ISO ha sostituito il *British Standard Occupational Health and Safety Assessment Series* - OHSAS 18001:2007).

La Società si è dotata, in relazione alla natura e dimensioni dell'organizzazione ed al tipo di attività svolta, di un'articolazione di funzioni che assicura, anche attraverso il presidio della Capogruppo, le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

In particolare, la Capogruppo presidia il ruolo di Responsabile del Servizio Prevenzione e Protezione (“RSPP”) ed in particolare collabora con il Datore di lavoro della Società nell'attività di valutazione di tutti i rischi per la sicurezza e salute sui luoghi di lavoro, nonché nell'elaborazione e aggiornamento del documento di valutazione dei rischi adottato dalla Società.

Le Unità Organizzative aziendali incaricate della gestione della documentazione inerente la materia, quali autorizzazioni/certificazioni/nullaosta rilasciati dalla Pubblica Amministrazione, sono tenute al rispetto dei principi di comportamento stabiliti e descritti nel protocollo “Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione”.

La politica aziendale in tema di salute e sicurezza sul lavoro deve essere diffusa, compresa, applicata ed aggiornata a tutti i livelli organizzativi, a tal fine vengono predisposti piani formativi adeguati e rispondenti alla normativa in materia, che tengano in considerazione il ruolo aziendale ricoperto, l'esposizione a specifici rischi e l'assegnazione di particolari incarichi per la gestione delle situazioni di emergenza. Le linee d'azione generali della Società devono essere orientate a un costante miglioramento della qualità della sicurezza e devono contribuire allo sviluppo effettivo di un “sistema di prevenzione e protezione”. Tutte le Unità Organizzative della Società devono osservare le disposizioni in materia di salute, di sicurezza e di igiene del lavoro e tenerne conto in occasione di qualsivoglia modifica degli assetti esistenti, compresi ristrutturazioni/allestimenti di siti operativi. Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di AFC Digital HUB, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

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

Descrizione del processo

Il processo di gestione dei rischi in materia di salute e sicurezza sul lavoro prevede le seguenti fasi:

- identificazione dei pericoli e loro classificazione (pericoli per la sicurezza e pericoli per la salute dei lavoratori);
- valutazione dei rischi;
- individuazione e predisposizione delle misure di prevenzione e di protezione;
- definizione di un piano di intervento con l'identificazione delle strutture aziendali competenti all'attuazione di detti interventi;
- realizzazione degli interventi pianificati nell'ambito di un programma;
- verifica dell'attuazione e controllo sull'efficacia delle misure adottate.

Con specifico riferimento alla gestione dei cantieri (artt. 88 e seguenti del Testo Unico) che è nella responsabilità del "Committente", il processo prevede le seguenti fasi:

- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi;
- designazione del Responsabile dei Lavori e, ove necessario, del Direttore dei Lavori, del Coordinatore per la progettazione e del Coordinatore per l'esecuzione dei lavori, previa verifica dei requisiti professionali dei soggetti incaricati, e formalizzazione per iscritto dei relativi incarichi;
- pianificazione delle fasi di lavorazione e loro valutazione con particolare riferimento alle interazioni delle attività interferenti anche al contorno del cantiere ed alla eventuale compresenza di attività della Società e predisposizione dei piani di sicurezza e coordinamento ovvero, ove non previsti dalla norma dei documenti di valutazione dei rischi interferenziali, anche per il tramite di professionisti incaricati;
- redazione delle lettere di richiesta di offerta con informativa alla controparte di quanto predisposto in tema di sicurezza (piani di sicurezza e coordinamento/documenti di valutazione dei rischi interferenziali);
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza, inerenti alle misure per gestire le interferenze, in relazione all'entità e alle caratteristiche del servizio/fornitura offerti nonché contenente dichiarazione di presa visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- esecuzione degli adempimenti tecnico-amministrativi, notifiche e comunicazioni alla Pubblica Amministrazione, anche per il tramite dei professionisti incaricati;
- aggiudicazione del servizio e stipula del contratto, con indicazione dei costi per la sicurezza e allegazione del piano di sicurezza e coordinamento/documento di valutazione dei rischi interferenziali;

- coordinamento nell'esecuzione delle attività fra le imprese/lavoratori autonomi e controlli sul rispetto delle misure nel cantiere, anche per il tramite dei professionisti incaricati.

Nei cantieri temporanei o mobili allestiti in unità operative ove sono presenti collaboratori della Società i rischi derivanti da interferenze tra le due attività sono gestiti dal Committente, anche per il tramite di professionisti all'uopo incaricati, individuando le specifiche misure di prevenzione, protezione ed emergenza a tutela della salute e sicurezza dei collaboratori, dei clienti e delle imprese appaltatrici e lavoratori autonomi. Tali misure sono indicate nel Piano di Sicurezza e Coordinamento o, ove non previsto, nel Documento unico di valutazione dei rischi interferenziali (in relazione al rispettivo campo di applicazione) elaborato a cura dei soggetti individuati dal Committente, che può avvalersi anche del supporto del sistema di prevenzione e protezione della Società.

Con specifico riferimento alla gestione dei contratti di appalto, contratti d'opera, contratti di somministrazione rientranti nell'ambito di applicazione dell'art. 26 del Testo Unico, il processo prevede le seguenti fasi:

- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi;
- informativa alla controparte circa i rischi specifici presenti nei luoghi in cui è chiamata ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla attività oggetto del contratto, nonché ove previsto dalla normativa, predisposizione del Documento di Valutazione dei Rischi Interferenziali (DUVRI), da inviare all'offerente ai fini della formulazione dell'offerta e parte integrante del contratto, contenente le misure idonee per eliminare o ridurre i rischi relativi alle interferenze delle attività connesse all'esecuzione del contratto e contestuale redazione della lettera di richiesta d'offerta ove prevista;
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza, inerenti alle misure per gestire le interferenze, in relazione all'entità e alle caratteristiche del servizio/fornitura offerti nonché contenente dichiarazione di presa di visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- aggiudicazione del servizio e stipula del contratto, con l'indicazione dei costi per la sicurezza e allegazione del DUVRI;
- esecuzione del servizio/fornitura da parte dell'aggiudicatario con espressa indicazione del personale dello stesso con funzione di Preposto, cooperazione e coordinamento con le imprese/lavoratori autonomi, per gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, anche mediante reciproca informazione al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva ed i rischi insiti nell'eventuale presenza di personale, collaboratori e clienti della Società;
- controllo sul rispetto degli adempimenti contrattuali nell'esecuzione delle attività.

Per gli adempimenti prescritti dal citato art. 26 del Testo Unico il Datore di Lavoro ha conferito apposita delega al Responsabile della funzione Immobili per le attività di competenza di tale funzione, che può prevedere ulteriore delega a soggetti specificatamente individuati.

Con specifico riferimento all'attività di sorveglianza sanitaria, il processo prevede le seguenti fasi:

- individuazione e nomina del Medico Competente;
- svolgimento della sorveglianza sanitaria:
 - pianificazione annuale dell'attività (visite mediche in scadenza e sopralluoghi degli ambienti di lavoro), condivisa con i Medici Competenti;
 - aggiornamenti periodici nel corso dell'anno e verifiche per valutare eventuali necessità di introdurre piani di miglioramento;
- elaborazione periodica di relazioni epidemiologiche sulla base dei dati anonimi relativi alla sorveglianza sanitaria; tale attività contribuisce alla valutazione e prevenzione di qualsiasi effetto negativo sulla salute e sul benessere dei lavoratori e, di conseguenza, anche all'individuazione/valutazione nel contesto lavorativo di fattori di rischio nuovi o non usuali.

Strettamente connessa alla sorveglianza sanitaria è la visita da parte del Medico Competente del luogo di lavoro ove opera il lavoratore. Il sopralluogo ha l'obiettivo di permettere una lettura integrata delle risultanze delle sopra indicate attività, di formulare giudizi di idoneità contestualizzati all'ambiente di lavoro e di suggerire specifiche eventuali ulteriori analisi sulla base di quanto emerso nel corso del sopralluogo.

Con specifico riferimento all'attività di analisi degli infortuni sul lavoro e delle malattie professionali, il processo prevede le seguenti fasi:

- attivazione di una istruttoria preliminare che consiste in una attività di verifica e approfondimento tramite la raccolta di tutti gli elementi conoscitivi sia di natura testimoniale sia documentale;
- effettuazione di un sopralluogo - se necessario - per individuare la causa primaria dell'evento;
- definizione degli eventuali provvedimenti correttivi da adottare.

Con specifico riferimento all'attività di valutazione dello stress lavoro correlato, il percorso metodologico scelto per la valutazione del rischio da stress lavoro-correlato si basa sull'attività di ricerca del Dipartimento di Medicina del Lavoro dell'ISPESL⁵⁰ e prevede le seguenti fasi:

- valutazione preliminare (necessaria/obbligatoria);
- valutazione approfondita (eventuale).

⁵⁰ Tale attività è ora confluita in INAIL: "Valutazione e gestione del rischio da stress lavoro-correlato. Manuale ed uso delle aziende in attuazione del Testo Unico e s.m.i."

La valutazione è effettuata da un “Gruppo di gestione della valutazione” che programma, coordina e applica l’intero processo. Il Gruppo è costituito - nel rispetto della previsione del Testo Unico da: i) Datore di Lavoro (e suoi delegati); ii) Responsabile Servizio Prevenzione e Protezione e Addetti del Servizio Prevenzione e Protezione; iii) Medici Coordinatori e Medici competenti. Tale Gruppo sente altresì i lavoratori e/o i Rappresentanti dei Lavoratori per la Sicurezza (allorquando presenti) e si avvale delle funzioni aziendali ritenute necessarie in relazione alle caratteristiche della Società nonché di eventuali consulenze di specialisti esterni.

Le procedure di gestione e di controllo del processo si basano su una chiara e formalizzata assegnazione di compiti e responsabilità con riferimento alle Strutture coinvolte (ivi compresi gli outsourcer esterni) nelle verifiche di conformità alle disposizioni tempo per tempo vigenti in tema di salute e sicurezza nonché su un coerente sistema di deleghe che disciplina le funzioni ed i poteri derivanti dagli obblighi normativi previsti dal Testo Unico.

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

Principi di controllo

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

- Livelli autorizzativi definiti nell’ambito del processo:
 - il sistema di gestione aziendale prevede la definizione di specifiche responsabilità al fine di consentire la piena attuazione della politica di salute e sicurezza sul lavoro con un approccio sistematico e pianificato. In particolare, sono state individuate le figure che rivestono il ruolo rispettivamente di “Datore di Lavoro” e “Committente”. Tali figure possono impartire disposizioni in materia alle Unità Organizzative aziendali, godendo della più ampia autonomia organizzativa e dispone dei più ampi poteri di spesa, anche con facoltà di delega e subdelega ai sensi dell’art. 16 comma 3 *bis* del Testo Unico;
 - è prevista un’articolazione di distinte funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
 - tutti i soggetti/figure aziendali che intervengono nelle fasi del processo sopra descritto devono essere individuati e autorizzati con espressa previsione della normativa interna o tramite delega interna, da conferirsi e conservarsi a cura del Datore di Lavoro e del Committente, ovvero a cura dei soggetti da costui facoltizzati.

- Segregazione dei compiti tra i differenti soggetti/figure coinvolte nel processo di gestione dei rischi in materia di salute e sicurezza sul lavoro. In particolare:

- le strutture che hanno il compito di realizzare e gestire gli interventi sono distinte e separate dalla struttura alla quale, per legge e/o normativa interna, sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
 - le Unità Organizzative competenti designano i soggetti ai quali sono attribuite specifiche mansioni per la gestione/prevenzione dei rischi per la sicurezza e la salute sul lavoro;
 - i Rappresentanti dei Lavoratori per la Sicurezza collaborano attivamente col Datore di Lavoro al fine di segnalare criticità ed individuare le conseguenti soluzioni.
- Attività di controllo:
 - La Società deve attivare un piano aziendale di controllo sistematico al fine di verificare periodicamente la corretta applicazione/gestione nonché l'efficacia delle procedure adottate e delle misure messe in atto per valutare, in ottemperanza alle prescrizioni di legge, i luoghi di lavoro. Il piano, in particolare, deve contemplare:
 - aree e attività aziendali da verificare (tra le quali le attività di natura organizzativa⁵¹, di sorveglianza sanitaria, di informazione e formazione dei lavoratori, di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori);
 - modalità di esecuzione delle verifiche, modalità di rendicontazione.

Il piano aziendale deve altresì assicurare:

- il rispetto degli *standard* tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- l'acquisizione di documentazioni e certificazioni obbligatorie di legge (relative ad edifici, impianti, ruoli, incarichi, abilitazioni, del personale e società, ecc.) da parte delle competenti Unità Organizzative;
- il rispetto del processo e degli adempimenti tecnici ed amministrativi previsti dalle normative interne e di legge.

Deve inoltre prevedere un idoneo sistema di controllo sulla sua efficace attuazione e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del piano devono essere adottati quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

- le Unità Organizzative competenti devono controllare che tutte le misure di prevenzione e protezione programmate siano attuate, assicurando un costante monitoraggio delle situazioni di rischio e dell'avanzamento dei programmi di intervento previsti dagli specifici documenti di valutazione dei rischi. La Società si avvale, laddove occorra, della collaborazione delle

⁵¹ Quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.

strutture della Capogruppo ovvero di società terze dalla stessa incaricate deputate alla gestione delle risorse umane, alla gestione e realizzazione di interventi immobiliari, di progettazione e gestione dei processi lavorativi, della sicurezza fisica, dei sistemi informativi, di gestione e manutenzione;

- i Rappresentanti dei Lavoratori per la Sicurezza, nel rispetto delle norme di legge in materia, possono accedere alla documentazione aziendale inerente la valutazione dei rischi e le misure di prevenzione relative e chiedere informazioni al riguardo. I medesimi Rappresentanti possono accedere ai luoghi di lavoro e formulare osservazioni in occasione di visite e verifiche da parte delle Autorità competenti;
- tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente, il Responsabile e gli addetti del Servizio Prevenzione e Protezione visitano i luoghi di lavoro;
- figure specialistiche di alta professionalità e con i titoli ed i requisiti previsti dalle norme specifiche preventivamente valutate, contribuiscono alla valutazione ed alla elaborazione di misure di tutela nel caso di rischi specifici in particolare:
 - il Medico Competente Coordinatore: incaricato dal Datore di Lavoro, garantisce gli adempimenti di sorveglianza sanitaria previsti dalla normativa, collabora con il Datore di Lavoro e con il Servizio Prevenzione e Protezione alla valutazione dei rischi, alla predisposizione dell'attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori; unifica ed aggiorna previa condivisione con i Medici Competenti Territoriali, i protocolli di sorveglianza sanitaria con le relative documentazioni e procedure;
 - Il Medico Competente Territoriale: incaricato dal Datore di Lavoro, per i territori di propria competenza, programma ed effettua la sorveglianza sanitaria attraverso protocolli sanitari definiti in funzione dei rischi specifici sulla base degli indirizzi generali forniti dal Medico Competente Coordinatore e del Documento di Valutazione dei Rischi ed esprime il giudizio di idoneità alla mansione specifica, comunicandone l'esito per iscritto al Datore di Lavoro ed al lavoratore;
 - il Responsabile del Rischio Amianto: viene designato in base al punto 4 del DM 06/09/94 con "compiti di controllo e coordinamento di tutte le attività manutentive che possono interessare i materiali in amianto". A tale riguardo coordina le attività di manutenzione che riguardano i MCA e supporta il Datore di Lavoro nel tenere idonea documentazione sull'ubicazione dei MCA; nel garantire il rispetto delle misure di sicurezza (per attività di pulizia, interventi di manutenzione e per ogni evento che possa causare un disturbo dei MCA); nel fornire agli occupanti dell'edificio una corretta informazione sulla presenza di amianto, sui potenziali rischi e sui comportamenti da adottare;

- l'Esperto di Radioprotezione: incaricato dal Datore di Lavoro, effettua le analisi e le valutazioni necessarie ai fini della sorveglianza fisica della protezione degli individui della popolazione;
 - l'Esperto abilitato in interventi di risanamento radon: fornisce le indicazioni tecniche ai fini dell'adozione delle misure correttive per la riduzione della concentrazione di radon negli edifici ai sensi dell'articolo 15 del D. Lgs.101/2010;
 - il Professionista antincendio: predispone pareri preventivi, istanze di valutazione dei progetti, certificazioni e dichiarazioni riguardanti gli elementi costruttivi, i prodotti, i materiali, le attrezzature, i dispositivi e gli impianti rilevanti ai fini della sicurezza antincendio;
- e nell'ambito dei cantieri (Titolo IV del Testo Unico):
- il Responsabile dei lavori: è incaricato dal Committente di svolgere i compiti attribuiti allo stesso dall'art. 90. Assorbe tutti i poteri e le responsabilità discendenti dall'obbligo giuridico di sorvegliare il cantiere, garantendo altresì che tutte le norme di sicurezza contenute nelle disposizioni in materia siano rispettate;
 - il Coordinatore per la progettazione: incaricato dal Committente o dal Responsabile nei casi previsti dalla legge. È deputato alla redazione del Piano di Sicurezza e Coordinamento (PSC);
 - il Coordinatore per l'esecuzione dei lavori: è chiamato a svolgere in cantiere non solo attività di coordinamento ma anche di controllo delle procedure di lavoro. I compiti del Coordinatore per l'esecuzione dei lavori tra l'altro riguardano la "validazione" del piano operativo di sicurezza, la verifica con opportune azioni di coordinamento e controllo, dell'applicazione, da parte delle imprese esecutrici, nonché dei lavoratori autonomi, delle disposizioni loro pertinenti contenute nel PSC e della corretta applicazione delle procedure di lavoro. Provvede inoltre alla sospensione dei lavori in caso di pericolo grave e imminente;
- le competenti strutture individuate dal Datore di Lavoro e dal Committente inoltre provvedono alla verifica dell'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare;
 - le competenti strutture individuate dal Committente verificano l'idoneità tecnico-professionale dei Responsabili dei Lavori e dei Coordinatori per la progettazione e per l'esecuzione, avute presenti anche le specifiche caratteristiche dei lavori oggetto di contratti di appalto;
 - qualora la documentazione prevista dal Testo Unico sia tenuta su supporto informatico, i competenti soggetti/unità operative verificano che le modalità di memorizzazione dei dati e di accesso al sistema di gestione della predetta documentazione assicurino quanto previsto dall'art. 53 del Testo Unico;
 - il Datore di Lavoro ed il Committente, ciascuno negli ambiti di competenza, vigilano ai sensi del comma 3 *bis* dell'art. 18 del Testo Unico in ordine all'adempimento degli obblighi in materia

- che la legge attribuisce a preposti, lavoratori, medici competenti, progettisti, fabbricanti, fornitori, installatori attraverso il piano aziendale di controllo sistematico sopra indicato;
- con riferimento ai cantieri temporanei o mobili, il Committente verifica il corretto conferimento degli incarichi e l'adempimento degli obblighi posti a carico del Direttore dei Lavori, del Responsabile dei Lavori, del Coordinatore per la progettazione e del Coordinatore per l'esecuzione dei lavori, ove nominati, nonché l'indicazione del nominativo Preposto dell'appaltatore; a tal fine acquisisce dagli stessi apposite relazioni periodiche che diano conto dell'attività svolta, delle eventuali criticità emerse e delle misure adottate per la loro soluzione;
 - le competenti Strutture individuate dal Datore di Lavoro e dal Committente, verificano il mantenimento nel tempo dei titoli e dei requisiti necessari per i Medici Competenti e degli specialisti che intervengono nei singoli processi;
 - il Preposto segnala alle competenti Strutture individuate dal Datore di Lavoro l'eventuale ritardo nell'adempimento delle prescrizioni del Medico Competente, per l'attivazione delle misure necessarie;
 - le competenti Strutture individuate dal Datore di Lavoro, verificano periodicamente la corretta gestione delle istruttorie preliminari condotte a fronte di infortunio sul luogo di lavoro.
- Tracciabilità del processo sia a livello di sistema informativo, sia in termini documentali:
 - l'impiego di sistemi per la gestione informatica dei dati e della documentazione prescritta dal Testo Unico deve avvenire nel rispetto dell'art. 53 del medesimo;
 - la Società, al fine di consentire la ricostruzione delle responsabilità, deve dotarsi di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività, ed è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rischi in materia di sicurezza e salute dei lavoratori nonché della relativa attività di controllo;
 - la Società è responsabile altresì dell'acquisizione, della conservazione e dell'archiviazione di documentazioni e certificazioni obbligatorie di legge e nonché della documentazione comprovante i requisiti tecnico-professionali delle imprese appaltatrici, dei lavoratori autonomi e dei soggetti destinatari di deleghe in materia di sicurezza (es.: Responsabile dei Lavori, Coordinatori per la progettazione e l'esecuzione).
 - la gestione dei diversi contesti di rischio prevede l'utilizzo di specifici sistemi informativi che consentano l'accesso in rete a tutte le Strutture interessate ed autorizzate alla valutazione dei rischi delle unità operative e che contengano, ad esempio, la documentazione tecnica di impianti, macchine, luoghi di lavoro, ecc., le liste degli esposti a specifici rischi, la documentazione sanitaria (con il rispetto dei requisiti di riservatezza previsti dalla normativa), le attività di formazione ed informazione, le attività di eliminazione/riduzione dei rischi, l'attività

ispettiva interna ed esterna, le informazioni in tema di infortuni e segnalazioni di rischio, la modulistica per la gestione dei monitoraggi ambientali e della cartella sanitaria, ecc..

Principi di comportamento

Le Unità Organizzative della Società, a qualsiasi titolo coinvolte nella gestione dei rischi in materia di salute e sicurezza sul lavoro, come pure tutto il personale, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare, tutte le Unità Organizzative sono tenute - nei rispettivi ambiti - a:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela e valutando la scelta delle attrezzature di lavoro nonché la sistemazione dei luoghi di lavoro;
- richiedere per i beni immobili e/o mobili oggetto di locazione finanziaria il rilascio di espresse dichiarazioni di conformità da parte dei soggetti titolati a renderle a norma di legge;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;
- astenersi dall'affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità qualificata e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice Interno di Comportamento di Gruppo;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es. Ispettorato del Lavoro, A.S.L., Vigili del Fuoco, ecc.) in occasione di accertamenti/procedimenti ispettivi;
- provvedere, nell'ambito dei contratti di somministrazione, appalto, d'opera o di fornitura, ad informare le controparti sui rischi specifici dell'ambiente in cui sono destinate ad operare e ad elaborare ed applicare le misure atte a governare in sicurezza le eventuali interferenze fra le imprese, compresi gli eventuali lavoratori autonomi, evidenziando nei contratti per i quali sia prescritto i costi per la sicurezza;
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- curare il rispetto delle normative in tema di salute e sicurezza nei confronti di tutto il personale, ivi compresi i lavoratori non dipendenti, con particolare riferimento all'ambito dei contratti regolati

dal D. Lgs. 81/2015 e successive modifiche ed integrazioni, nonché nei confronti dei soggetti beneficiari di iniziative di tirocinio e dei terzi in genere che dovessero trovarsi nei luoghi di lavoro;

- assicurarsi che, nell'impiego di sistemi di elaborazione automatica dei dati, le modalità di memorizzazione dei dati e di accesso al sistema di gestione della documentazione prescritta garantiscano quanto previsto dall'art. 53 del Testo Unico.

Parimenti, tutto il Personale è tenuto a:

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dai soggetti/unità operative e dalle Autorità competenti;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- segnalare immediatamente ai soggetti/figure competenti, ogni situazione di pericolo potenziale o reale, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tale situazione di pericolo.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti (anche omissivi) che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001.

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

7.7 Area sensibile concernente i reati informatici e di indebito utilizzo di strumenti di pagamento diversi dai contanti

7.7.1 Fattispecie di reato

Premessa

Sezione I – Reati Informatici

La legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa, stipulata a Budapest il 23.11.2001, avente quale obiettivo la promozione della cooperazione internazionale tra gli Stati firmatari al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici, specie in considerazione della natura di tali illeciti, che spesso, nelle modalità della loro preparazione o realizzazione, coinvolgono Paesi diversi.

La riforma della disciplina della criminalità informatica è stata realizzata sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti. L'art. 7 della legge ha inoltre aggiunto al D. Lgs. 231/2001 l'art. 24-*bis*, che elenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli Enti.

La citata legge ha modificato anche il codice di procedura penale, e le disposizioni in tema di protezione dei dati personali, essenzialmente al fine di agevolare le indagini sui dati informatici e consentire per determinati periodi la conservazione dei dati relativi al traffico telematico. Non sono invece state recepite nell'ordinamento italiano le definizioni di "sistema informatico" e di "dato informatico" contenute nella Convenzione di Budapest; tali definizioni, che si riportano qui di seguito, potranno essere prese come riferimento dalla giurisprudenza in materia:

- "sistema informatico": qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati;
- "dato informatico": qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

L'art. 24-*bis* del D. Lgs. 231/2001 individua i reati informatici che – nella materia della criminalità informatica, fondata su disposizioni di matrice comunitaria – possono dar luogo alla responsabilità amministrativa degli enti.

Si illustrano qui di seguito i reati presupposto elencati dall'art. 24 *bis* del Decreto.

Accesso abusivo ad un sistema telematico o informatico (art. 615 *ter* c.p.)

Il reato è commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo.

Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici. Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell'interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema.

Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della Società (o anche di terzi concesse in licenza alla Società), mediante l'utilizzo delle credenziali di altri colleghi abilitati.

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

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.)

La condotta punita dall'art. 617 *quater* c.p. consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento o interruzione delle stesse. Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni.

L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di *software* (c.d. ad esempio spyware). L'impedimento od interruzione delle comunicazioni (c.d. "*Denial of service*") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime comunicazioni fittizie.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema.

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

L'art. 617 *quinquies* punisce chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica,

consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti a intercettare, impedire o interrompere dette comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

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

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 *ter* c.p.)

L'art. 635 *bis* c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui. Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.

L'art. 635 *ter* c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.

Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio.

Qualora le condotte descritte conseguano ad un accesso abusivo al sistema esse saranno punite ai sensi del sopra illustrato art. 615 *ter* c.p.

Danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.)

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinqüies* c.p.)

L'art. 635 *quater* c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 *bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.

L'art. 635 *quinqüies* c.p. punisce le medesime condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra

espressamente fra gli “eventi” aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità.

In questa previsione, a differenza di quanto previsto all’art. 635 *ter*, non vi è più alcun riferimento all’utilizzo da parte di enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente “di pubblica utilità”; non sarebbe cioè, da un lato, sufficiente l’utilizzo da parte di enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.

Entrambe le fattispecie sono perseguibili d’ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. È da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento.

Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615 *ter* c.p.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all’accesso a sistemi informatici o telematici (art. 615 *quater* c.p.)

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.)

L’art. 615 *quater* punisce chiunque al fine di procurare a sé od ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all’accesso di un sistema informatico o telematico, protetto da misure di sicurezza o comunque fornisce indicazioni idonee al predetto scopo.

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

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

La prima fattispecie richiede che il reo agisca a scopo di lucro o di altrui danno. Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del

carattere obiettivamente abusivo di trasmissioni di dati, programmi, e-mail, etc., da parte di chi, pur non essendo mosso da specifica finalità di lucro o di causazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

Falsità nei documenti informatici (art. 491 bis c.p.)

L'art. 491 bis c.p. dispone che ai documenti informatici pubblici aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nell'attribuibilità allo stesso di un'efficacia probatoria secondo le norme civilistiche⁵².

Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato (anche da parte dell'autore originario) successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate.

Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione.

Non sembrano poter trovare applicazione, con riferimento ai documenti informatici, le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487, 488 c.p.). Il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità.

⁵² Si rammenta al riguardo che, ai sensi del Codice dell'amministrazione digitale (cfr. art. 1, lettera p) del D.Lgs. 82/2005), il documento informatico è "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", ma:

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

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.)

Tale reato è commesso dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato⁵³. Il soggetto attivo del reato può essere soltanto un soggetto “certificatore qualificato”, che esercita particolari funzioni di certificazione per la firma elettronica qualificata.

A tale specifico proposito si osserva che la Società non riveste tuttavia la qualifica di “certificatore qualificato”.

Ostacolo alle procedure in tema di definizione, gestione e controllo del “Perimetro di sicurezza nazionale cibernetica” (art. 1, comma 11 D.L. n. 105/2019)

Il reato punisce chi, allo scopo di ostacolare o condizionare le Autorità preposte a tutelare il sistema delle infrastrutture tecnologiche strategiche:

- 1) fornisce informazioni, dati o elementi di fatto non rispondenti al vero rilevanti:
 - a) per la predisposizione e aggiornamento degli elenchi delle reti, dei sistemi (comprensivi della relativa architettura e componentistica) e dei servizi informatici della Pubblica Amministrazione e degli operatori pubblici e privati con sede in Italia, dai quali dipende l’esercizio di una funzione essenziale dello Stato o la prestazione di servizio essenziale per le attività civili, sociali o economiche fondamentali e dal cui malfunzionamento, interruzione o abuso possa derivare un pericolo per la sicurezza nazionale;
 - b) ai fini delle comunicazioni che detti operatori pubblici e privati devono effettuare al CVCN (Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello Sviluppo economico) dei contratti di fornitura che intendano stipulare per approvvigionarsi di beni, sistemi e servizi ICT destinati a essere impiegati nelle reti, sistemi e servizi di cui al punto che precede;
 - c) per lo svolgimento delle attività ispettive e di vigilanza concernenti il rispetto delle disposizioni e procedure inerenti alla predisposizione e aggiornamento dei predetti elenchi, alla comunicazione delle forniture e alla notifica degli incidenti e alle misure di sicurezza relative ai sopra menzionati, sistemi, reti e servizi;
- 2) omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

A tale specifico proposito, la Società non rientra tra i soggetti tenuti al rispetto degli obblighi di cui al D.L. n. 105/2019.

⁵³ Per certificato qualificato si intende, ai sensi dell’art. 1 lettere e) ed f) del D. Lgs. 82/2005, l’attestato elettronico che collega all’identità del titolare i dati utilizzati per verificare le firme elettroniche, che sia conforme ai requisiti stabiliti dall’allegato I della direttiva 1999/93/CE, rilasciato da certificatori - vale a dire i soggetti che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi con quest’ultime - che rispondono ai requisiti di cui all’allegato II della medesima direttiva.

* * *

Sezione II – Reati in materia di strumenti di pagamento diversi dai contanti

Il Decreto legislativo 184/2021 ha introdotto nel catalogo dei reati presupposto della responsabilità dell'ente⁵⁴ i delitti in materia di strumenti di pagamento diversi dai contanti inserendo: l'aggravante di cui all'art. 640 *ter*, comma 2, c.p., le modifiche all'art. 493 *ter* c.p. e, ex novo, l'art. 493 *quater* c.p. Caratteristiche e contesto di detti reati fanno sì che gli stessi possano essere ricondotti nell'Area sensibile dei reati informatici fermo che, anche in questo caso, le attività sensibili previste in quest'area, ricomprendente reati che possono generare proventi illeciti, si devono intendere predisposte anche al fine della prevenzione dei reati di riciclaggio in senso lato.

Si illustrano di seguito i reati introdotti dall'art. 25 *octies*.1:

Frode informatica che produce trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640 *ter*, comma 2).

La fattispecie, come già visto nel paragrafo dedicato ai reati contro la Pubblica Amministrazione, consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati, informazioni o programmi in essi contenuti, ottenendo un ingiusto profitto. La circostanza aggravante che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale determina anche la responsabilità dell'Ente senza bisogno che il soggetto passivo sia lo Stato, la Pubblica Amministrazione o l'UE.

Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (493 *ter* c.p.)

La fattispecie punisce la condotta di chi, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti.

Viene punita anche la condotta di chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Il rischio di commissione di tale reato può in teoria configurarsi in tutte le realtà aziendali ed in particolare in tutti i processi aziendali interessati dalla movimentazione di flussi finanziari, in relazione alle differenti tipologie di strumenti di pagamento diverse dai contanti.

In particolare sono sensibili tutte le attività che rendono possibile l'accesso a dati identificativi, credenziali, etc., funzionali all'eventuale utilizzo indebito di strumenti di pagamento (diversi dai contanti) di titolarità di terzi, quali ad esempio le carte di credito.

⁵⁴ Cfr art. 25 *octies*.1 D. Lgs. 231/2001.

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 *quater* c.p.)

Salvo che il fatto costituisca più grave reato, la fattispecie punisce chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a se' o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

La condotta descritta potrebbe riscontrarsi nell'ambito di quelle attività che comportano la gestione e/o la diffusione di strumenti di pagamento diversi dai contanti e negli ambienti tecnologici a supporto di dette attività.

L'articolo 25 *octies*.1 del D. Lgs. 231/2001, ha inoltre esteso il catalogo dei reati presupposto a "ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale" a condizione che ne siano oggetto materiale "strumenti di pagamento diversi dai contanti".

* * *

In generale può osservarsi che alcune fattispecie di reati informatici in concreto potrebbero non presentare il requisito della commissione nell'interesse o a vantaggio della Società, indispensabile affinché possa conseguire la responsabilità amministrativa della stessa. Per altro verso si ricorda che qualora fossero integrati tutti gli elementi previsti dal Decreto la responsabilità della Società potrebbe sorgere, secondo la previsione contenuta nell'art. 8 del Decreto, anche quando l'autore del reato non sia identificabile (dovrebbe quantomeno essere provata la provenienza della condotta da un soggetto apicale o da un dipendente, anche se non identificato), evenienza tutt'altro che improbabile nel campo della criminalità informatica, in ragione della complessità dei mezzi impiegati e dell'evanescenza del cyberspazio, che rendono assai difficile anche l'individuazione del luogo ove il reato stesso possa ritenersi consumato.

Va infine ricordato che l'art. 640 *ter* c.p., che punisce il delitto di frode informatica, costituiva già reato presupposto della responsabilità amministrativa degli Enti ex art.24 D. Lgs. 231/2001 se perpetrata ai danni dello Stato o di altro ente pubblico; al riguardo si rimanda al paragrafo 7.2.1.

7.7.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio di commissione dei reati informatici (ivi compresi i reati di "Frode informatica che produce trasferimento di denaro, di valore monetario o di valuta virtuale" e "Detenzione e diffusione di apparecchiature, dispositivi o programmi

informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti) e di trattamento illecito di dati attengono alla gestione e all'utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo, attività pertanto connesse a ogni ambito aziendale che utilizza le tecnologie dell'informazione.

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

- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo.

Infine per quanto attiene il reato di Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti ed ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale, a condizione che ne siano oggetto materiale strumenti di pagamento diversi dai contanti, le attività aziendali sensibili della Società nelle quali può essere commessa questa tipologia di reato, riguardano tutti i processi aziendali che comportano la movimentazione di flussi finanziari della Società attraverso le differenti tipologie di strumenti di pagamento diverse dai contanti e dei relativi applicativi.

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

- Gestione e utilizzo degli strumenti di pagamento diversi dai contanti.

Si evidenzia altresì che nell'ambito di protocolli che regolano altre attività sensibili quali la Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali (paragrafo 7.2.2.6) sono previsti alcuni principi di controllo e di comportamento che esplicano la loro efficacia preventiva anche in relazione ai suddetti reati.

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

7.7.2.1 Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative coinvolte nella gestione ed utilizzo di sistemi informatici e del Patrimonio Informativo di Gruppo.

Le attività inerenti la gestione e utilizzo dei sistemi informativi e del Patrimonio Informativo di Gruppo sono svolte con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere.

In particolare, si applica:

- nella gestione e nell'utilizzo dei sistemi informativi che si interconnettono/utilizzano *software* della Pubblica Amministrazione ovvero delle Autorità di Vigilanza;
- nella progettazione, nella realizzazione o gestione di strumenti informatici, tecnologici o di telecomunicazioni;
- nella realizzazione di interventi di tipo organizzativo, normativo e tecnologico per garantire la protezione del Patrimonio Informativo di Gruppo nelle attività connesse con il proprio mandato e nelle relazioni con i terzi che accedono al Patrimonio Informativo del Gruppo;
- a tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzano i sistemi informativi della Società e trattano i dati del Patrimonio Informativo di Gruppo.

Ai sensi del D. Lgs. 231/2001, i relativi processi potrebbero presentare occasioni per la commissione dei delitti informatici contemplati dall'art. 24-*bis* nonché dei reati di "*Frode informatica*" previsto dall'art. 640 *ter* del codice penale e richiamato dagli artt. 24 e 25 *octies.1* del Decreto e "*Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti*". Inoltre, mediante l'accesso alle reti informatiche potrebbero essere integrate le condotte illecite aventi ad oggetto le opere dell'ingegno protette⁵⁵.

Si rileva come la Società utilizzi sistemi informatici della Capogruppo, sviluppati e coordinati da quest'ultima. Le misure di sicurezza per l'integrità dei dati e dei sistemi sono stabilite principalmente mediante specifiche *policy* di Gruppo.

Quanto definito dal presente protocollo è volto a garantire il rispetto della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

⁵⁵ Cfr. "Area sensibile concernente i reati contro l'industria e il commercio, i reati in materia di violazione del diritto d'autore e i reati doganali".

Descrizione del processo

L'utilizzo e la gestione di sistemi informatici e del Patrimonio Informativo sono attività imprescindibili per l'espletamento del *business* aziendale e contraddistinguono la maggior parte dei processi della Società.

Gli eventuali adempimenti verso la Pubblica Amministrazione che prevedano il ricorso a specifici programmi forniti dagli stessi Enti, ovvero la connessione diretta con gli stessi, sono espletati mediante le attrezzature di proprietà della Capogruppo che assicura un'efficace e stringente definizione di norme e misure di sicurezza organizzative, comportamentali e tecnologiche e la realizzazione di attività di controllo, peculiari del presidio a tutela di una gestione e di un utilizzo dei sistemi informatici e del Patrimonio Informativo della Società in coerenza con la normativa vigente. Il processo di gestione dei sistemi informatici e del Patrimonio Informativo di Gruppo si articola nelle seguenti fasi fondamentali:

- analisi del rischio IT e definizione dei requisiti di sicurezza informatica;
- gestione Accessi Risorse Informatiche e Servizi di Sicurezza ICT;
- gestione normativa e architettura di sicurezza informatica;
- monitoraggio eventi sicurezza informatica e gestione eventi critici di sicurezza informatica;
- sicurezza delle terze parti (classificazione e monitoraggio dei fornitori);
- diffusione della cultura di sicurezza informatica;
- progettazione e realizzazione soluzioni di sicurezza informatica.

Il processo di prevenzione frodi si articola nelle seguenti fasi:

- identificazione delle misure atte al rafforzamento della prevenzione;
- monitoraggio dell'evoluzione delle frodi informatiche, anche per quanto riguarda eventuali aspetti di sicurezza fisica correlati;
- presidio delle attività necessarie all'intercettazione e alla soluzione delle minacce verso gli asset aziendali;
- gestione delle comunicazioni con le Forze dell'Ordine.

Il processo di gestione della sicurezza fisica si articola nelle seguenti fasi:

- gestione protezione di aree e locali ove si svolge l'attività;
- gestione sicurezza fisica dei sistemi periferici (ambienti di filiali, sede centrale, altre reti).

Il processo relativo al servizio di certificazione di firma elettronica si articola nelle seguenti fasi:

- apertura del contratto;
- registrazione del titolare;

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

Il processo relativo alla progettazione, sviluppo e attivazione dei servizi ICT si articola nelle seguenti fasi:

- progettazione, realizzazione e gestione delle soluzioni applicative e delle infrastrutture tecnologiche di Gruppo;

Il processo di gestione e supporto ICT si articola nelle seguenti fasi:

- erogazione dei servizi ICT;
- monitoraggio del funzionamento dei servizi ICT e gestione delle anomalie;
- assistenza agli utenti attraverso attività di Help desk e problem solving.

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

Principi di controllo

Fatti salvi i requisiti di sicurezza propri del *software* della Pubblica Amministrazione o delle Autorità di Vigilanza eventualmente utilizzati, il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
 - i soggetti coinvolti nel processo devono essere appositamente incaricati;
 - la gestione delle abilitazioni avviene tramite la definizione di "profili di accesso" in ragione delle funzioni svolte all'interno della Società anche tramite la competente struttura dell'*outsourcer*; le variazioni al contenuto dei profili sono eseguite dalle competenti strutture dell'*outsourcer* DSI deputate al presidio della sicurezza logica, su richiesta della Società;
 - le variazioni al contenuto dei profili sono eseguite dalle strutture della Società deputate al presidio della sicurezza logica, su richiesta delle strutture interessate. La struttura richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative coperte;
 - ogni utente ha associato un solo profilo abilitativo in relazione al proprio ruolo aziendale nel rispetto del principio del minimo privilegio. In caso di trasferimento o di modifica dell'attività dell'utente, viene attribuito il profilo abilitativo corrispondente al nuovo ruolo assegnato.
- Segregazione dei compiti:
 - sono assegnati distinti ruoli e responsabilità di gestione della sicurezza delle informazioni; in particolare:

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

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

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

- l'adeguata formazione del personale sugli aspetti di sicurezza per sviluppare una maggiore sensibilità;
- la predisposizione e l'aggiornamento delle norme di sicurezza, al fine di garantirne nel tempo l'applicabilità, l'adeguatezza e l'efficacia;
- i controlli sulla corretta applicazione ed il rispetto della normativa definita.

Le principali attività di controllo, tempo per tempo effettuate, e specificamente dettagliate nella normativa interna di riferimento, sono le seguenti:

Con riferimento alla sicurezza fisica:

- protezione e controllo delle aree fisiche (perimetri/zone riservate) in modo da scongiurare accessi non autorizzati, alterazione o sottrazione degli asset informativi.

Con riferimento alla sicurezza logica:

- identificazione e autenticazione dei codici identificativi degli utenti;
- autorizzazione relativa agli accessi alle informazioni richiesti;
- previsione di tecniche crittografiche e di firma digitale per garantire la riservatezza, l'integrità e il non ripudio delle informazioni archiviate o trasmesse.

Con riferimento all'esercizio ed alla gestione di applicazioni, sistemi e reti:

- previsione di una separazione degli ambienti (sviluppo, collaudo e produzione) nei quali i sistemi e le applicazioni sono installati, gestiti e mantenuti in modo tale da garantire nel tempo la loro integrità e disponibilità;
- predisposizione e protezione della documentazione di sistema relativa alle configurazioni, personalizzazioni e procedure operative, funzionale ad un corretto e sicuro svolgimento delle attività;
- previsione di misure per le applicazioni in produzione in termini di installazione, gestione dell'esercizio e delle emergenze, protezione del codice, che assicurino il mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni trattate;
- attuazione di interventi di rimozione di sistemi, applicazioni e reti individuati come obsoleti;
- pianificazione e gestione dei salvataggi di sistemi operativi, software, dati e delle configurazioni di sistema;
- gestione delle apparecchiature e dei supporti di memorizzazione per garantire nel tempo la loro integrità e disponibilità tramite la regolamentazione ed il controllo sull'utilizzo degli strumenti, delle apparecchiature e di ogni asset informativo in dotazione nonché mediante la definizione di modalità di custodia, riutilizzo, riproduzione, distruzione e trasporto fisico dei supporti rimovibili di memorizzazione delle informazioni, al fine di proteggerli da danneggiamenti, furti o accessi non autorizzati;

- monitoraggio di applicazioni e sistemi, tramite la definizione di efficaci criteri di raccolta e di analisi dei dati relativi, al fine di consentire l'individuazione e la prevenzione di azioni non conformi;
- prevenzione da software dannoso tramite sia opportuni strumenti ed infrastrutture adeguate (tra cui i sistemi antivirus) sia l'individuazione di responsabilità e procedure per le fasi di installazione, verifica di nuovi rilasci, aggiornamenti e modalità di intervento nel caso si riscontrasse la presenza di software potenzialmente dannoso;
- formalizzazione di responsabilità, processi, strumenti e modalità per lo scambio delle informazioni tramite posta elettronica e siti web;
- adozione di opportune contromisure per rendere sicura la rete di telecomunicazione e gli apparati a supporto e garantire la corretta e sicura circolazione delle informazioni;
- previsione di specifiche procedure per le fasi di progettazione, sviluppo e cambiamento dei sistemi e delle reti, definendo i criteri di accettazione delle soluzioni;
- previsione di specifiche procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge e contrattuali.

Con riferimento allo sviluppo ed alla manutenzione delle applicazioni:

- individuazione di opportune contromisure ed adeguati controlli per la protezione delle informazioni gestite dalle applicazioni, che soddisfino i requisiti di riservatezza, integrità e disponibilità delle informazioni trattate, in funzione degli ambiti e delle modalità di utilizzo, dell'integrazione con i sistemi esistenti e del rispetto delle disposizioni di Legge e della normativa interna;
- previsione di adeguati controlli di sicurezza nel processo di sviluppo delle applicazioni, al fine di garantirne il corretto funzionamento anche con riferimento agli accessi alle sole persone autorizzate, mediante strumenti, esterni all'applicazione, per l'identificazione, l'autenticazione e l'autorizzazione.

Con riferimento alla gestione degli incidenti di sicurezza:

- previsione di opportuni canali e modalità di comunicazione per la tempestiva segnalazione di incidenti e situazioni sospette al fine di minimizzare il danno generato e prevenire il ripetersi di comportamenti inadeguati e attivare l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi.

● Tracciabilità del processo:

- il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;

- tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente, ecc.), con particolare riguardo all'operato di utenze con privilegi speciali, risultano tracciate attraverso sistematica registrazione (sistema di log files);
- tutti i transiti in ingresso e in uscita degli accessi alle zone riservate, del solo personale che ne abbia effettiva necessità previa debita autorizzazione, sono rilevati tramite appositi meccanismi di tracciatura;
- è prevista la tracciatura delle attività effettuate sui dati, compatibili con le leggi vigenti al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate.

Principi di comportamento

Le strutture, a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e del Patrimonio Informativo di Gruppo sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- la Società deve predisporre e mantenere il censimento degli eventuali applicativi che si interconnettono con la Pubblica Amministrazione o con le Autorità di Vigilanza e/o dei loro specifici *software* in uso;
- i soggetti coinvolti nel processo devono essere appositamente incaricati;
- il personale/ogni amministratore del sistema è tenuto alla segnalazione alla Direzione aziendale di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di *hacker* esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente ed attivando l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi;
- il personale è responsabile del corretto utilizzo delle risorse informatiche assegnategli (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- qualora sia previsto il coinvolgimento di soggetti terzi/*outsourcer* nella gestione dei sistemi informatici e del Patrimonio Informativo di Gruppo nonché nell'interconnessione/utilizzo dei *software* della Pubblica Amministrazione o delle Autorità di Vigilanza, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni

caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate o di utilizzare indebitamente, falsificare o alterare strumenti di pagamento diversi dai contanti;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società o del Gruppo, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti *software* non autorizzati (virus, worm, trojan, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o ad altri apparecchiature, dispositivi o programmi informatici progettati principalmente per commettere reati riguardanti strumenti di pagamento diversi dai contanti o adattati a tale scopo;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;

- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:
 - diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurpare la paternità;
 - abusivamente duplicare, detenere o diffondere in qualsiasi forma programmi per elaboratore od opere audiovisive o letterarie;
 - detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;
 - riprodurre banche di dati su supporti non contrassegnati dalla SIAE, diffonderle in qualsiasi forma senza l'autorizzazione del titolare del diritto d'autore o in violazione del divieto imposto dal costituente;
 - rimuovere o alterare informazioni elettroniche inserite nelle opere protette o compresenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;
 - importare, promuovere, installare, porre in vendita, modificare o utilizzare, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

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

7.7.2.2 Gestione e utilizzo degli strumenti di pagamento diversi dai contanti

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative della Società coinvolte nella gestione e nell'utilizzo degli strumenti di pagamento diversi dai contanti.

Le attività aziendali che implicano la gestione e l'utilizzo di strumenti di pagamento diversi dal contante sono svolte con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere.

Ai sensi del D. Lgs 231/2001, il processo potrebbe presentare occasioni per la commissione del reato di *"Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti"* e ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale a condizione che ne siano oggetto materiale strumenti di pagamento diversi dai contanti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del Processo

Il processo di gestione e utilizzo degli strumenti di pagamento diversi dai contanti si articola nei seguenti processi:

- Gestione di Incassi e pagamenti (es., per quanto applicabile, assegni, bonifici addebiti diretti, RIBA – MAV – effetti etc.);
- Gestione delle risorse Umane con riferimento alle carte di credito aziendali, ai buoni pasto, alle carte di servizio per le autovetture (carta carburante, strumenti di ricarica elettrica, telepass) rilasciate agli eventuali dipendenti della Società o del Gruppo.

Le modalità operative per la gestione dei processi descritti sono disciplinate, in tutto o in parte, nell'ambito della normativa anche di Gruppo applicabile, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti. In particolare:
 - i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione dei rapporti contrattuali inerenti il protocollo in oggetto sono individuati e autorizzati in base allo specifico ruolo loro attribuito dal funzionigramma aziendale ovvero dal Responsabile della Struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima.

- Segregazione dei compiti:
 - sono attribuite precise responsabilità nella gestione del processo di gestione:
 - delle carte di pagamento – comprese le carte di credito aziendali – attraverso la definizione di compiti e controlli specifici in merito alle attività di richiesta, consegna, sostituzione, rinnovo, attivazione, revoca, rinuncia o recesso dell'eventuale dipendente;
 - degli assegni (richiesta o ottenimento, gestione degli adempimenti in caso di smarrimento, sottrazione e distruzione degli stessi).
- Attività di controllo:
 - adozione di misure organizzative e tecnologiche atte alla prevenzione e contrasto delle condotte che possano portare ad un indebito utilizzo degli strumenti di pagamento, diversi dal contante, in uso presso la Società.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo di gestione e utilizzo degli strumenti di pagamento diversi dai contanti;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, le Strutture – di volta in volta interessate nella gestione degli strumenti di pagamento diversi dai contanti – sono responsabili dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente all'esecuzione degli adempimenti svolti nell'ambito della gestione delle attività sopra descritte.

Principi di comportamento

Le Strutture, a qualsiasi titolo coinvolte nelle attività di gestione e di utilizzo degli strumenti di pagamento diversi dai contanti sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare:

- i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione dei rapporti contrattuali devono essere appositamente incaricati;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dei sistemi di pagamento diversi dai contanti, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;

- tutti i dipendenti devono segnalare immediatamente qualunque tentativo di falsificazione ed indebito utilizzo di strumenti finanziari diversi dai contanti di cui dovessero venire a conoscenza e deve immediatamente segnalarla secondo le modalità previste dal paragrafo 4.1.

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

- utilizzare indebitamente e/o favorire l'utilizzo indebito da parte di terzi che non ne sono titolari di carte di pagamento, ovvero di qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque di ogni altro strumento di pagamento diverso dai contanti;
- falsificare o alterare gli strumenti di pagamento diversi dai contanti,
- possedere, cedere o acquisire strumenti di pagamento diversi dai contanti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi;
- introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di utilizzare indebitamente, falsificare o alterare strumenti di pagamento diversi dai contanti.

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

7.8 Area sensibile concernente i reati contro l'industria e il commercio, i reati in materia di violazione del diritto d'autore e i reati doganali⁵⁶

7.8.1 Fattispecie di reato

Premessa

La L. 23.7.2009 n. 99 – Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in tema di energia – in un più ampio quadro di iniziative di rilancio dell'economia e di tutela del “*Made in Italy*”, dei consumatori e della concorrenza, ha attratto nell'ambito della responsabilità da reato degli Enti numerose norme penali, alcune delle quali dalla stessa legge emanate o riformulate. In particolare, nel testo del D. Lgs. 231/2001, gli artt. 25-*bis* e 25-*bis*.1 richiamano fattispecie previste dal codice penale in tema di industria e di commercio⁵⁷, mentre l'art. 25-*novies* – al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno⁵⁸ e i gravi danni economici arrecati agli autori e all'industria connessa – rimanda a reati contemplati dalla legge sul diritto d'autore (L. n. 633/1941).

Alle predette disposizioni si aggiungono i reati di contrabbando⁵⁹, introdotti nell'articolo 25-*sexiesdecies*⁶⁰ al fine di recepire le disposizioni della legislazione europea poste a tutela degli interessi della finanza pubblica dell'Unione Europea.

Si descrivono qui di seguito gli illeciti in questione.

Contraffazione, alterazione o uso di marchi o di segni distintivi ovvero di brevetti, modelli e disegni di prodotti industriali (art. 473 c.p.)

La norma punisce le condotte di chi, pur potendo accertare l'altrui appartenenza di marchi e di altri segni distintivi di prodotti industriali, ne compie la contraffazione, o altera gli originali, ovvero fa uso dei marchi falsi senza aver partecipato alla falsificazione⁶¹.

Integrano la contraffazione le ipotesi consistenti nella riproduzione identica o nell'imitazione degli elementi essenziali del segno identificativo, in modo tale che ad una prima percezione possa apparire autentico. Si tratta di quelle falsificazioni materiali idonee a ledere la pubblica fiducia circa

⁵⁶ La possibilità di commissione dei reati doganali, tenuto conto dell'operatività della Società, è stata ritenuta ragionevolmente remota.

⁵⁷ A seguito della modifica apportata dalla L. 99/2009, l'art. 25-*bis* del D. Lgs. 231/2001 - che in precedenza riguardava i soli ai reati di falsità in materia di monete e di valori di bollo - concerne anche i delitti previsti dagli articoli 473 e 474 Cod. Pen., i quali hanno in comune con i primi il bene giuridico principalmente tutelato e cioè la fede pubblica, intesa quale affidamento che la generalità dei cittadini ripone nella veridicità di determinati oggetti, segni o attestazioni.

⁵⁸ Ai sensi dell'art. 1 della L. 633/1941 sono tutelate le opere dell'ingegno di carattere creativo che appartengono alla letteratura (anche scientifica o didattica), alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma d'espressione. Sono altresì protetti come opere letterarie i programmi per elaboratore nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

⁵⁹ La possibilità di commissione dei reati doganali, tenuto conto dell'operatività della Società, è stata ritenuta ragionevolmente remota.

⁶⁰ Cfr. l'articolo 5 del D. Lgs. 75/2020

⁶¹ Per “fare uso” dei marchi falsi dovrebbero intendersi condotte residuali, quali ad esempio l'apposizione su propri prodotti di marchi falsificati da terzi. Si deve trattare cioè di condotte diverse sia dalla messa in circolazione di prodotti recanti marchi falsi previste nell'art. 474 c.p., sia dalle condotte più propriamente realizzative della contraffazione, quale ad esempio la riproduzione del marchio altrui nelle comunicazioni pubblicitarie, nella corrispondenza commerciale, nei siti internet, ecc.

la provenienza di prodotti o servizi dall'impresa che è titolare, licenziataria o cessionaria del marchio registrato. Secondo la giurisprudenza è tutelato anche il marchio non ancora registrato, per il quale sia già stata presentata la relativa domanda, in quanto essa lo rende formalmente conoscibile. È richiesto il dolo, che potrebbe sussistere anche qualora il soggetto agente, pur non essendo certo dell'esistenza di altrui registrazioni (o domande di registrazione), possa dubitarne e ciononostante non proceda a verifiche.

Il secondo comma sanziona le condotte di contraffazione, nonché di uso da parte di chi non ha partecipato alla falsificazione, di brevetti, disegni e modelli industriali altrui⁶². Anche questa disposizione intende contrastare i falsi materiali che, nella fattispecie, potrebbero colpire i documenti comprovanti la concessione dei brevetti o le registrazioni dei modelli. La violazione dei diritti di esclusivo sfruttamento economico del brevetto è invece sanzionata dall'art. 517-ter c.p.

Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

L'art. 474 c.p. punisce le condotte di coloro che, estranei ai reati di cui all'art. 473 c.p., introducono in Italia prodotti industriali recanti marchi o segni distintivi contraffatti o alterati, oppure detengono per la vendita, mettono in vendita o comunque in circolazione prodotti contraffatti, sempre che non siano già punibili per l'introduzione in Italia. È sempre richiesto il fine di trarre profitto.

Il detentore potrebbe essere punito, oltre che per il reato in questione, anche a titolo di ricettazione, qualora fosse a conoscenza fin dal momento dell'acquisto della falsità dei segni distintivi apposti ai prodotti dal suo fornitore o da altri. Si ricorda che, ai sensi dell'art. 25-*octies* del Decreto, anche il reato di ricettazione può dar luogo alla responsabilità amministrativa degli enti.

Turbata libertà dell'industria e del commercio (art. 513 c.p.)

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

Illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.)

Commette questo delitto l'imprenditore che compie atti di concorrenza con violenza o minaccia. La norma, introdotta nel codice penale dalla legge antimafia "Rognoni – La Torre" n. 646/1982, trova applicazione anche al di fuori della criminalità mafiosa ed intende contrastare gli atti diretti a impedire

⁶² Il Codice della proprietà industriale (D.Lgs. 30/2005), all'art. 2 recita: "La brevettazione e la registrazione danno luogo ai titoli di proprietà industriale. Sono oggetto di brevettazione le invenzioni, i modelli di utilità, le nuove varietà vegetali. Sono oggetto di registrazione i marchi, i disegni e modelli, le topografie dei prodotti a semiconduttori".

o limitare l'intervento sul mercato di operatori concorrenti. Il reato sussiste anche quando la violenza o la minaccia sia posta in essere da terzi per conto dell'imprenditore, oppure non sia direttamente rivolta al concorrente, ma ai suoi potenziali clienti. Potrebbe ad esempio ravvisarsi il reato nelle ipotesi di: minaccia di arrecare un danno ingiusto diretta ai partecipanti a una gara pubblica al fine di conoscere le loro offerte e formularne più basse; minaccia, nel rapporto con un proprio cliente, di applicare condizioni peggiorative o di revocare i crediti concessi, ovvero, nel rapporto con un proprio fornitore, di non effettuare altri ordini nel caso in cui il cliente/fornitore ricorra ai servizi di/fornisca un determinato concorrente.

Frodi contro le industrie nazionali (art. 514 c.p.)

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

Frode nell'esercizio del commercio (art. 515 c.p.)

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

Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)

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

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)

Il delitto consiste nel mettere in vendita o comunque in circolazione opere dell'ingegno o prodotti industriali con nomi, marchi o segni distintivi⁶³ atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto. È sufficiente che i segni distintivi, anche in relazione alle altre circostanze del caso concreto (prezzi dei prodotti, loro caratteristiche, modalità della vendita) possano ingenerare nel comune consumatore confusione con i prodotti affini (ma diversi per origine, provenienza o qualità) contrassegnati dal marchio genuino. La norma tutela l'onestà nel commercio e si applica sussidiariamente, quando non ricorrano gli estremi delle più gravi incriminazioni degli artt. 473 e 474 c.p. In essa ricadono casi quali la contraffazione e l'utilizzo di marchi non registrati, l'uso di recipienti o di confezioni con marchi originali, ma contenenti prodotti diversi, l'uso da parte del legittimo titolare del proprio marchio per contraddistinguere prodotti con

⁶³ L'art. 181-bis, comma 8, della L. n. 633/1941 dispone che ai fini della legge penale il contrassegno SIAE è considerato segno distintivo di opera dell'ingegno.

standard qualitativi diversi da quelli originariamente contrassegnati dal marchio (il caso non ricorre se la produzione sia commissionata ad altra azienda, ma il committente controlli il rispetto delle proprie specifiche qualitative).

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)

Il reato consta di due diverse fattispecie. La prima, perseguibile a querela, punisce chiunque, potendo conoscere dell'esistenza di brevetti o di registrazioni altrui, fabbrica o utilizza ai fini della produzione industriale oggetti o altri beni, usurpando un titolo di proprietà industriale o in violazione dello stesso. Qualora sussista la falsificazione dei marchi o un'altra delle condotte previste dagli artt. 473 e 474 c.p., l'usurpatore potrebbe rispondere anche di tali reati.

La seconda fattispecie concerne la condotta di chi, al fine di trarne profitto, introduce in Italia, detiene per la vendita, pone in vendita o mette comunque in circolazione beni fabbricati in violazione dei titoli di proprietà industriale. Se le merci sono contraddistinte da segni falsificati si applica anche l'art. 474, comma 2, c.p.

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)

Le condotte punite consistono nell'apporre a prodotti agroalimentari false o alterate indicazioni geografiche o denominazioni d'origine⁶⁴ nonché, ai fini di trarne profitto, nell'introdurre in Italia, detenere per la vendita, porre in vendita o mettere comunque in circolazione i medesimi prodotti con indicazioni o denominazioni contraffatte.

Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941)

Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941)

Commette il primo delitto in esame chiunque, senza averne il diritto, a qualsiasi scopo ed in qualsiasi forma, mette a disposizione del pubblico un'opera dell'ingegno protetta o parte di essa, immettendola in un sistema di reti telematiche mediante connessioni di qualsiasi genere. In alcuni particolari casi - per finalità culturali o di libera espressione ed informazione e con determinate limitazioni - è consentita la comunicazione al pubblico di opere altrui⁶⁵.

Il secondo delitto in oggetto consiste nell'abusivo utilizzo dell'opera dell'ingegno altrui (mediante riproduzione, trascrizione, diffusione in qualsiasi forma, commercializzazione, immissione in reti telematiche, rappresentazione o esecuzione in pubblico, elaborazioni creative, quali le traduzioni, i

⁶⁴ Ai sensi dell'art. 29 del D. Lgs. 30/2005 sono protette: "le indicazioni geografiche e le denominazioni di origine che identificano un paese, una regione o una località, quando siano adottate per designare un prodotto che ne è originario e le cui qualità, reputazione o caratteristiche sono dovute esclusivamente o essenzialmente all'ambiente geografico d'origine, comprensivo dei fattori naturali, umani e di tradizione".

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

compendi, ecc.) aggravato dalla lesione dei diritti morali dell'autore. Alla condotta di per sé già abusiva deve cioè aggiungersi anche la violazione del divieto di pubblicazione imposto dall'autore, o l'usurpazione della paternità dell'opera (c.d. plagio), ovvero la sua deformazione, mutilazione, o altra modificazione che offenda l'onore o la reputazione dell'autore.

Entrambe le incriminazioni si applicano in via residuale, quando non risulti presente il dolo specifico del fine di trarre un profitto od un lucro, che deve invece caratterizzare le condotte, in parte identiche, più severamente sanzionate dagli artt. 171-*bis* e 171-*ter*.

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

Il primo comma della norma, con riferimento ai programmi per elaboratore⁶⁶, punisce le condotte di abusiva duplicazione, nonché di importazione, distribuzione, vendita, detenzione a scopo commerciale od imprenditoriale (quindi anche per uso limitato all'ambito della propria impresa), concessione in locazione, quando hanno per oggetto programmi contenuti in supporti privi del contrassegno della società italiana degli autori ed editori (SIAE). Costituiscono inoltre reato l'approntamento, la detenzione o il traffico di qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione da utilizzi abusivi dei programmi.

Il secondo comma, con riferimento alla tutela dei diritti dell'autore di una banca di dati⁶⁷, punisce la riproduzione - permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma - su supporti non contrassegnati dalla SIAE, il trasferimento su altro supporto, la distribuzione, la comunicazione, la presentazione o la dimostrazione in pubblico non autorizzate dal titolare del diritto d'autore. Sono altresì sanzionate le condotte di estrazione e di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati, in violazione del divieto imposto dal costituente⁶⁸ della medesima banca dati. Per estrazione deve intendersi il trasferimento di dati permanente o temporaneo su un altro supporto con qualsiasi mezzo o in qualsivoglia forma e per reimpiego qualsivoglia forma di messa a disposizione del pubblico dei dati mediante distribuzione di copie, noleggio, trasmissione con qualsiasi mezzo e in qualsiasi forma.

Tutte le predette condotte devono essere caratterizzate dal dolo specifico del fine di trarre profitto, vale a dire di conseguire un vantaggio, che può consistere anche solo in un risparmio di spesa.

⁶⁶ Ai sensi dell'art. 2, n. 8, della L. n. 633/1941 sono tutelati i programmi per elaboratore in qualsiasi forma espressi purché originali, quale risultato di creazione intellettuale dell'autore. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso. Gli artt. 64-*bis*, 64-*ter* e 64-*quater* della citata legge disciplinano l'estensione dei diritti che competono all'autore del programma e i casi di libera utilizzazione dello stesso, vale a dire le ipotesi in cui sono consentite riproduzioni od interventi sul programma anche senza specifica autorizzazione del titolare dei diritti.

⁶⁷ Ai sensi dell'art. 2, n. 9, della L. n. 633/1941, le banche di dati consistono in raccolte di opere, dati od altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici od in altro modo. Resta ovviamente salva la distinta tutela riconosciuta ai diritti d'autore eventualmente esistenti sulle opere dell'ingegno inserite nella banca dati. Gli artt. 64-*quinquies* e 64-*sexies* della legge disciplinano l'estensione dei diritti dell'autore della banca di dati nonché i casi di libera utilizzazione della stessa.

⁶⁸ I diritti del costituente sono regolati dagli artt. 102-*bis* e 102-*ter* della L. n. 633/1941. Per costituente si intende colui che effettua investimenti rilevanti per la creazione, la verifica o la presentazione di una banca di dati ed al quale compete, indipendentemente dalla tutela che spetta al suo autore in ordine ai criteri creativi secondo i quali il materiale è stato scelto ed organizzato, il diritto di vietare le operazioni di estrazione o di reimpiego della totalità o di una parte sostanziale del contenuto della banca dati. Per le banche di dati messe a disposizione del pubblico, ad esempio mediante libero accesso on line, gli utenti, anche senza espressa autorizzazione del costituente, possono effettuare estrazioni o reimpieghi di parti non sostanziali, valutate in termini qualitativi e quantitativi, per qualsivoglia fine, salvo che l'estrazione od il reimpiego siano stati espressamente vietati o limitati dal costituente.

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

La norma elenca una nutrita casistica di condotte illecite - se commesse per uso non personale e col fine di lucro - aventi ad oggetto: opere destinate al circuito televisivo, cinematografico, della vendita o del noleggio; supporti di qualunque tipo contenenti opere musicali, cinematografiche, audiovisive, loro fonogrammi, videogrammi o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche, didattiche, musicali, multimediali. Sono infatti punite:

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

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

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

Commettono il reato i produttori od importatori di supporti contenenti *software* destinati al commercio che omettono di comunicare alla SIAE i dati necessari all'identificazione dei supporti per i quali vogliono avvalersi dell'esenzione dall'obbligo di apposizione del contrassegno SIAE⁶⁹.

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

⁶⁹ L'art. 181-bis, comma 3, della L. n. 633/1941 dispone che, fermo restando il rispetto dei diritti tutelati dalla legge, possono essere privi del contrassegno SIAE i supporti contenenti *software* da utilizzarsi esclusivamente tramite elaboratore elettronico, che non contengano opere audiovisive intere non realizzate espressamente per il programma per elaboratore, ovvero riproduzioni di parti eccedenti il 50% di preesistenti opere audiovisive, che diano luogo a concorrenza nell'utilizzazione economica delle stesse.

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

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

Reati di contrabbando (D. Lgs. 43/1973).

Tali norme puniscono un'articolata serie di condotte che, in estrema sintesi, sono accomunate dallo scopo di sottrarre merci al pagamento dei diritti di confine dovuti.

Per diritti di confine si intendono i dazi di importazione e di esportazione, i prelievi e le altre imposizioni alle esportazioni o importazioni previsti da regolamenti comunitari, i diritti di monopolio, le sovrimposte di confine e ogni altra imposta o sovrimposta di consumo a favore dello Stato.

7.8.2 Attività aziendali sensibili

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

- nell'approvvigionamento e utilizzo di prodotti, software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società o destinati ad omaggi;
- nello sviluppo (anche tramite *partner* esterni), ingegnerizzazione e messa a disposizione di terzi o dei soci (ad esempio tramite concessione della licenza d'uso) di algoritmi "anti-frode".

Meno rilevante appare il rischio con riferimento alle attività di gestione del naming e dei marchi del Gruppo, della comunicazione esterna o pubblicitaria e delle iniziative di marketing, nonché con riferimento alle attività di gestione dei rapporti con le controparti.

Si rimanda pertanto ai protocolli:

- "Stipula e gestione dei rapporti contrattuali con le controparti, ivi inclusa la Pubblica Amministrazione", disciplinata al paragrafo 7.2.2.1;
- "Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali" disciplinata al paragrafo 7.2.2.6;
- "Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo" disciplinata al paragrafo 7.7.2.1;

che contengono principi di controllo e di comportamento che esplicano la loro efficacia preventiva anche in relazione ai reati suddetti.

Relativamente ai reati di contrabbando⁷⁰, i rischi di commissione dei medesimi possono presentarsi più verosimilmente rispetto alle seguenti attività sensibili a cui si rimanda:

- “Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali” (in caso di eventuale acquisto di beni oggetto di importazione), disciplinata al paragrafo 7.2.2.6;
- “Gestione delle attività inerenti la richiesta di autorizzazioni o l’esecuzione di adempimenti verso la Pubblica Amministrazione” (in caso di gestione di adempimenti nei confronti dell’Amministrazione doganale), disciplinata al paragrafo 7.2.2.2;

i cui protocolli contengono principi di controllo e di comportamento che esplicano la loro efficacia preventiva anche in relazione ai reati suddetti.

Detti protocolli si applicano anche a presidio delle attività svolte, sulla base di appositi contratti di servizio, dalla Capogruppo e/o *outsourcer* esterni.

⁷⁰ La possibilità di commissione dei reati di contrabbando, tenuto conto dell’operatività della Società, è stata ritenuta ragionevolmente remota.

7.9 Area sensibile concernente i reati ambientali

7.9.1 *Fattispecie di reato*

Premessa

L'art. 25-*undecies* del D. Lgs. 231/2001 individua gli illeciti dai quali, nella materia della tutela penale dell'ambiente, fondata su disposizioni di matrice comunitaria, discende la responsabilità amministrativa degli enti⁷¹.

Si tratta di reati descritti nel codice penale, nel D. Lgs. 152/2006 (Codice dell'ambiente, per brevità nel seguito C. A.) e in varie leggi speciali, sia di natura delittuosa, puniti in presenza di dolo, sia di tipo contravvenzionale⁷².

Le fattispecie sono le seguenti.

Inquinamento ambientale (art. 452-*bis* c.p.)

La norma punisce chi cagiona abusivamente una compromissione o un deterioramento significativi e misurabili delle acque, dell'aria, del suolo o del sottosuolo, di un ecosistema o della biodiversità.

Disastro ambientale (art. 452-*quater* c.p.)

La norma punisce chi abusivamente provoca un disastro ambientale, che consiste nell'alterazione dell'equilibrio di un ecosistema che sia irreversibile, o la cui eliminazione sia particolarmente onerosa ed eccezionale, oppure nell'offesa all'incolumità pubblica, in ragione della gravità del fatto, per estensione, o per gli effetti, o per il numero di persone offese o esposte a pericolo.

Delitti colposi contro l'ambiente (art. 452-*quinquies* c.p.)

La norma punisce chi commette a titolo di colpa le fattispecie di inquinamento ambientale e disastro ambientale, operando una diminuzione di pena. È prevista una ulteriore diminuzione di pena qualora non venga cagionato un vero e proprio inquinamento o disastro ambientale, ma un mero pericolo, da accertarsi in concreto.

Traffico e abbandono di materiale ad alta radioattività (art. 452-*sexies* c.p.)

Sono punite molteplici condotte abusive (cessione, acquisto, ricezione, trasporto, importazione, esportazione, detenzione, abbandono, ecc.) concernenti materiali ad alta radioattività.

⁷¹ L'art. 25 *undecies* del D. Lgs. 231/2001, in vigore dal 16 agosto 2011, nel testo dapprima inserito dal D. Lgs. 121/2011, emanato in recepimento delle Direttive 2008/99/CE e 2009/123/CE, e successivamente modificato dalla L. 68/15, in vigore dal 29 maggio 2015, che ha introdotto nel codice penale i nuovi delitti contro l'ambiente.

⁷² Le fattispecie delittuose sono quelle previste dal codice penale (eccetto gli artt. 727 *bis* e 733 *bis*) e dal C.A. agli artt. 258, comma 4, 2° periodo, 260, c. 1 e 2, 260 *bis*, commi 6, 7 e 8, nonché i reati di falsi documentali in tema di commercio di specie animali e vegetali e il reato di inquinamento doloso provocato da navi. Di regola, le fattispecie contravvenzionali sono punite anche se commesse a titolo di colpa; i delitti di inquinamento e disastro ambientale, se commessi per colpa, sono puniti ai sensi dell'art. 452 *quinquies* codice penale e costituiscono anch'essi reati presupposto della responsabilità amministrativa degli enti.

Associazione a delinquere con aggravante ambientale (art. 452-octies c.p.)

La norma prevede una specifica aggravante di pena per i reati di associazione a delinquere aventi lo scopo di commettere taluno dei delitti ambientali previsti dal codice penale. Se si tratta di reato di associazione mafiosa, costituisce aggravante il fatto stesso dell'acquisizione della gestione o del controllo di attività economiche, di concessioni, autorizzazioni, appalti o di servizi pubblici in materia ambientale.

Reati concernenti specie animali o vegetali selvatiche protette o habitat protetti (artt. 727-bis e 733-bis c.p.)

Sono punite le condotte di prelievo, possesso, uccisione o distruzione di esemplari appartenenti a specie animali o vegetali selvatiche protette, fuori dei casi consentiti dalla legge e salvo che si tratti di danni considerati trascurabili, per quantità di esemplari o per impatto sullo stato di conservazione della specie. È altresì punita la condotta di distruzione o di deterioramento tale da compromettere lo stato di conservazione di un habitat situato all'interno di un sito protetto. Le norme comunitarie elencano le specie animali o vegetali protette e individuano le caratteristiche che impongono la classificazione da parte della legge nazionale di un habitat naturale o di specie come zona a tutela speciale o zona speciale di conservazione.

Violazioni della disciplina degli scarichi (art. 137, commi 2, 3, 5, 11 e 13, C. A.)

L'art. 137 C. A. punisce una serie di violazioni della disciplina degli scarichi ed in particolare: gli scarichi senza autorizzazione di acque reflue industriali contenenti determinate sostanze pericolose, oppure in difformità delle prescrizioni dell'autorizzazione o nonostante la sua sospensione o revoca, nonché gli scarichi di sostanze pericolose oltre i valori limite; le violazioni dei divieti di scarico sul suolo, nelle acque sotterranee e nel sottosuolo fuori dalle ipotesi ammesse dagli artt. 103 e 104 C.A..

Infine, sono sanzionate le violazioni dei divieti di scarichi in mare effettuati da navi o aerei di sostanze pericolose previste dalle convenzioni internazionali, salvo che si tratti di scarichi autorizzati di quantità rapidamente biodegradabili.

Violazioni della disciplina sulla gestione dei rifiuti (art. 256, commi 1, 3, 5 e comma 6, 1° periodo, C.A.)

Le condotte punite consistono nella raccolta, trasporto, recupero, smaltimento commercio o intermediazione di rifiuti senza le prescritte autorizzazioni, iscrizioni all'Albo nazionale gestori ambientali e comunicazioni alle competenti Autorità, oppure in difformità delle disposizioni contenute nelle autorizzazioni o impartite dalle Autorità o in carenza dei requisiti prescritti.

Sono altresì punite le attività di realizzazione o gestione di una discarica non autorizzata, di miscelazione di rifiuti pericolosi di diverso genere tra di loro o con rifiuti non pericolosi e di deposito di rifiuti sanitari pericolosi presso il luogo di produzione, per quantitativi superiori a 200 litri o equivalenti.

Omissione di bonifica per i casi di inquinamento del suolo, del sottosuolo, delle acque superficiali o sotterranee (art. 257, commi 1 e 2, C.A.)

Salvo che il fatto non costituisca più grave reato (ad es. quello di cui sopra all'art. 452-*bis* c.p.) è punito chi avendo cagionato l'inquinamento in oggetto con il superamento delle concentrazioni soglia di rischio non provvede alle dovute comunicazioni alle competenti Autorità e alla bonifica del sito ai sensi dell'art. 242 C.A. L'effettuazione della bonifica costituisce condizione di non punibilità anche per le contravvenzioni ambientali previste da altre leggi speciali per il medesimo evento.

Falso in certificato di analisi rifiuti (art. 258, comma 4, 2° periodo, C. A.)⁷³

Commette il delitto in questione chi fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti riportate in un certificato di analisi dei rifiuti e chi utilizza il certificato falso per il trasporto dei rifiuti.

Traffico illecito di rifiuti (art. 259, comma 1, C. A.)

La norma punisce chi effettua una spedizione di rifiuti transfrontaliera in violazione del Regolamento CE n. 259/93, che peraltro è stato abrogato e sostituito dal Regolamento CE n. 1013/2006.

Attività organizzate per il traffico illecito di rifiuti (art. 452 – *quaterdecies*, commi 1 e 2 c.p.)

Tale delitto è commesso da chi, al fine di conseguire un ingiusto profitto, cede, riceve, trasporta, esporta, importa o comunque gestisce abusivamente ingenti quantitativi di rifiuti. Deve trattarsi di fatti non episodici, ma di attività continuative, per lo svolgimento delle quali siano stati predisposti appositi mezzi ed organizzazione. È prevista un'aggravante di pena per il caso di rifiuti altamente radioattivi.

Falsità nella tracciabilità dei rifiuti mediante il SISTRI (art. 260-*bis*, comma 6 – comma 7, 2° e 3° periodo - comma 8, C. A.)⁷⁴

Al sistema informatico di controllo della tracciabilità dei rifiuti, denominato SISTRI, partecipano obbligatoriamente o su base volontaria, secondo i criteri di cui all'art. 188-*ter* C.A., i produttori di

⁷³ L'art. 4 del D. Lgs. n. 116/2020 ha riformulato l'art. 258 C.A. a far tempo dal 26 settembre 2020, con la conseguenza che il secondo periodo del quarto comma a cui tuttora rimanda l'art. 25-*undecies* del D. Lgs. 231/2001 prevede una fattispecie diversa, concernente il trasporto di rifiuti pericolosi senza formulario, mentre quella qui descritta ora è collocata nel terzo periodo del medesimo comma. Si ritiene pertanto che a causa della svista del legislatore possa sostenersi che né la nuova fattispecie né quella originaria possano costituire reato presupposto.

⁷⁴ A decorrere dal 1.1.2019 il SISTRI è stato abolito dall'art. 6 del D.L. 135/2018, che introduce un nuovo sistema di tracciabilità dei rifiuti, meglio definito dal D. Lgs. n. 116/2020 (il cosiddetto "REN") la cui disciplina attuativa deve essere ancora completata.

rifiuti e gli altri soggetti che intervengono nella loro gestione (commercianti, intermediari, consorzi di recupero o riciclaggio, soggetti che compiono operazioni di recupero o di smaltimento, trasportatori). In tale contesto sono puniti i delitti consistenti nel fornire false indicazioni sulla natura e sulle caratteristiche di rifiuti al fine della predisposizione di un certificato di analisi dei rifiuti da inserire in SISTRI, nell'inserire nel sistema un certificato falso o nell'utilizzare tale certificato per il trasporto dei rifiuti.

È altresì punito il trasportatore che accompagna il trasporto con una copia cartacea fraudolentemente alterata della scheda SISTRI compilata per la movimentazione dei rifiuti.

Violazioni della disciplina delle emissioni in atmosfera (art. 279, comma 5, C. A.)

La norma punisce le emissioni in atmosfera compiute nell'esercizio di uno stabilimento, superiori ai valori limite stabiliti dalla legge o fissati nelle autorizzazioni o prescrizioni delle competenti Autorità, quando siano superati anche i valori limite di qualità dell'aria previsti dalla vigente normativa.

Violazioni in tema di commercio e detenzione di animali o vegetali in via di estinzione o di mammiferi e rettili pericolosi (L. 150/1992, art. 1, commi 1 e 2 – art. 2, commi 1 e 2 – art. 3-bis comma 1 - art. 6, comma 4)

Gli illeciti consistono nell'importazione, esportazione, trasporto, detenzione di esemplari di animali o di vegetali in violazione delle disposizioni comunitarie e internazionali che impongono particolari autorizzazioni, licenze e certificazioni doganali, e nella falsificazione o alterazione dei predetti documenti. È vietata altresì la detenzione di determinati mammiferi e rettili pericolosi.

Sostanze lesive dell'ozono stratosferico (L. 549/1993, art. 3, comma 6)

La legge vieta il commercio, l'utilizzo, l'importazione, l'esportazione, la detenzione di sostanze lesive dell'ozono atmosferico dalla stessa elencate.

Inquinamento provocato dalle navi (D. Lgs. 202/2007, artt. 8 e 9)

La norma sanziona i comandanti delle navi, i membri dell'equipaggio, i proprietari e gli armatori che dolosamente o colposamente sversano in mare idrocarburi o sostanze liquide nocive trasportate alla rinfusa, fatte salve le deroghe previste.

7.9.2 Attività aziendali sensibili

Con riferimento all'operatività della Società, i rischi di commissione dei reati ambientali possono presentarsi più verosimilmente nella gestione degli adempimenti legislativi previsti in materia di smaltimento di rifiuti e alla manutenzione dei locali utilizzati.

Di seguito si riporta il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia ambientale.

Si rimanda inoltre ai seguenti protocolli, i quali contengono principi di controllo e principi di comportamento atti a prevenire anche la commissione dei reati di cui alla presente area sensibile:

- Gestione delle attività inerenti la richiesta di autorizzazioni o all'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali.

Detti protocolli si applicano anche a presidio delle attività svolte, sulla base di appositi contratti di servizio, dalla Capogruppo e/o *outsourcer* esterni.

7.9.2.1 Gestione dei rischi in materia ambientale

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative coinvolte nella gestione dei rischi in materia ambientale.

Le attività inerenti all'eventuale gestione dei rischi in materia ambientale sono svolte con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere.

Coerentemente col proprio Codice Etico che individua la tutela dell'ambiente tra i propri valori di riferimento, il Gruppo Intesa Sanpaolo ha adottato una specifica politica ambientale ed energetica che deve essere diffusa, compresa e applicata a tutti i livelli organizzativi.

Inoltre, il Gruppo Intesa Sanpaolo ha adottato e mantiene attivo un Sistema di Gestione Ambientale e dell'Energia, verificato annualmente da un Organismo di Certificazione Internazionale, conforme alle leggi vigenti e al più avanzato *standard* di riferimento: UNI EN ISO 14001 e UNI CEI EN ISO 50001.

Il Gruppo si è dotato, in relazione alla natura e dimensioni dell'organizzazione ed al tipo di attività svolta, di un'articolazione di funzioni che assicura le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

Le Unità Organizzative incaricate della gestione della documentazione inerente la materia ambientale, quali autorizzazioni e certificazioni rilasciate dalla Pubblica Amministrazione, sono tenute al rispetto dei principi di comportamento stabiliti e descritti nel protocollo "Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Descrizione del processo

La gestione dei rischi in materia ambientale si concretizza per la Società nella gestione degli adempimenti normativi in tema di rifiuti, di manutenzione dei locali utilizzati dalla stessa nonché nella selezione dei fornitori.

Principi di controllo

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

- Livelli autorizzativi definiti nell'ambito del processo:
 - il conferimento dell'incarico a fornitori spetta esclusivamente a soggetti muniti di idonee facoltà in base al vigente sistema di poteri e deleghe;

- la normativa interna illustra i meccanismi autorizzativi sottostanti l'affidamento di lavori in appalto/sub-appalto e il conferimento di incarichi relativi alla gestione dei rifiuti;
 - ogni trasporto di rifiuti speciali deve essere accompagnato da un formulario d'identificazione sottoscritto dal trasportatore e, per quanto attiene alla Società, da soggetti appositamente incaricati;
 - l'eventuale affidamento a terzi - da parte dei fornitori della Società - di attività in sub-appalto, è contrattualmente subordinato a un preventivo assenso da parte della Società ed al rispetto degli specifici obblighi sul rispetto della normativa ambientale.
- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi di gestione dei rischi in materia ambientale. In particolare:
 - le strutture che hanno il compito di realizzare e di gestire gli interventi quali servizi alle persone, servizi all'edificio ed altri servizi integrati (es.: fornitura toner, verifica/ricondizionamento/smaltimento dei materiali o prodotti informatici, ecc.) sono distinte e separate dalle strutture alle quali sono attribuiti compiti di consulenza in tema di valutazione dei rischi ambientali e di controllo sulle misure atte a prevenirli e a ridurli.
 - Attività di controllo:
 - Il formulario d'identificazione dei rifiuti speciali compilato e sottoscritto dal trasportatore deve essere verificato dal soggetto incaricato dalla Società;
 - verifica a campione sulla corretta gestione dei rifiuti con particolare riguardo a quelli speciali e, se presenti, a quelli pericolosi da parte delle funzioni competenti;
 - verifica sulla corretta gestione da parte dell'appaltatore dei rifiuti derivanti dalle attività di manutenzione ordinaria e straordinaria e da ristrutturazioni immobiliari. In particolare, l'appaltatore è tenuto a ritirare a propria cura gli "scarti" dal proprio ciclo di lavoro e i Responsabili o soggetti all'uopo incaricati devono vigilare sul corretto operato degli appaltatori evitando l'abbandono presso i locali dei rifiuti prodotti;
 - controllo sul corretto espletamento, da parte dei fornitori, dei servizi di manutenzione/pulizia (Servizi all'Edificio, Servizi alle Persone, ecc.) dei locali, con particolare riguardo alla regolare tenuta dei libretti d'impianto per la climatizzazione nonché ai report manutentivi periodici redatti dai fornitori che hanno in appalto i servizi suddetti.
 - Tracciabilità del processo:
 - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;

- documentabilità di ogni attività inerente ai processi con particolare riferimento alla corretta tenuta e conservazione dei libretti d'impianto per la climatizzazione secondo quanto previsto dalla normativa vigente, specie relativamente alle loro emissioni;
- conservazione nei termini di legge dei formulari d'identificazione dei rifiuti speciali (tre anni dalla data di emissione) e del registro di carico e scarico dei rifiuti pericolosi per i tre anni successivi dalla data dell'ultima registrazione;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, le strutture competenti sono responsabili dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente all'esecuzione degli adempimenti svolti nell'ambito dei processi sopra descritti.

Principi di comportamento

Le strutture, a qualsiasi titolo coinvolte nella gestione dei rischi in materia ambientale oggetto del protocollo come pure tutto il personale, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di Gruppo.

In particolare, tutte le strutture coinvolte sono tenute, nei rispettivi ambiti di competenza, a:

- vigilare, per quanto di competenza, sul rispetto degli adempimenti in materia ambientale, in particolare sull'osservanza delle norme operative riguardanti il raggruppamento e il deposito temporaneo dei rifiuti secondo la loro classificazione, sulla consegna ai trasportatori autorizzati, sulla conservazione nei termini di legge della documentazione amministrativa (Formulari di Identificazione dei Rifiuti e, ove applicabile, del Registro di Carico e Scarico);
- vigilare, per quanto di competenza, sul rispetto degli adempimenti in materia ambientale, in particolare sulla gestione di caldaie/centrali termiche, di gruppi frigoriferi/pompe di calore e di impianti di produzione di energia elettrica da sistemi di emergenza;
- astenersi dall'affidare incarichi/appalti a consulenti esterni e/o fornitori eludendo criteri documentabili e obiettivi incentrati su professionalità qualificata, competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal Codice interno di comportamento di Gruppo;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia ambientale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;
- prevedere, nell'ambito dei contratti di appalto, d'opera e di fornitura di Servizi alle Persone, Servizi all'Edificio, manutenzioni edili, opere edilizie/impiantistiche ed altri servizi integrati (es.: fornitura toner, verifica/ricondizionamento/smaltimento dei materiali o prodotti informatici, ecc.) specifiche clausole sul rispetto della normativa ambientale;

- nell'ambito delle procedure acquisitive di prodotti, macchine e attrezzature a fini strumentali, che a fine ciclo vita potrebbero essere classificati potenzialmente pericolosi per l'ambiente, le strutture committenti e la funzione acquisti competente devono ottenere preventivamente dal potenziale fornitore la "scheda di sicurezza/pericolosità del prodotto" ed i codici EER⁷⁵ e tutte le informazioni necessarie da utilizzare per il corretto smaltimento degli stessi;
- considerare come requisito rilevante per la valutazione del fornitore, ove la natura della fornitura lo renda possibile e opportuno, le certificazioni ambientali;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es, A.S.L., Vigili del Fuoco, ARPA, Comune, Provincia, ecc.) in occasione di accertamenti / procedimenti ispettivi.

Parimenti, tutto il personale è tenuto a:

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle strutture aziendali e dalle Autorità competenti;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, qualsiasi situazione di emergenza ambientale (es. sversamenti di gasolio, gravi malfunzionamenti degli impianti che provocano rumore esterno oltre i valori limite).

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- depositare i rifiuti al di fuori dal "Deposito Temporaneo Rifiuti" e consegnare i rifiuti speciali così come definiti dalla vigente normativa interna a fornitori incaricati del trasporto che non siano censiti nell'elenco delle Società autorizzate alla gestione dei rifiuti presente sulla intranet aziendale.

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

⁷⁵ EER - Elenco Europeo Rifiuti,

7.10 Area sensibile concernente i reati tributari

7.10.1 Fattispecie di reato

Premessa

La responsabilità degli enti è estesa ad alcuni dei reati in materia di imposte sui redditi e sul valore aggiunto previsti dal D. Lgs. n. 74/2000, che detta la disciplina di portata generale sui reati tributari, riformata per rafforzare la repressione del fenomeno dell'evasione fiscale e per recepire le disposizioni della legislazione europea poste a tutela degli interessi della finanza pubblica dell'UE. Le nuove fattispecie in materia tributaria sono state inserite nell'articolo 25-*quinquiesdecies* (reati tributari)⁷⁶. Si descrivono qui di seguito gli illeciti in questione.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D. Lgs. 74/2000)

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

Il primo reato è commesso da chi presenta dichiarazioni relative alle imposte sui redditi o all'IVA che indichino elementi passivi fittizi, risultanti da fatture o da altri documenti registrati nelle scritture contabili obbligatorie o conservati a fini di prova. Le fatture o i documenti utilizzati sono connotati da falsità materiale o ideologica circa l'esistenza in tutto o in parte delle operazioni in essi indicati, o circa il soggetto controparte.

Il secondo reato sussiste allorché, al di fuori del caso di uso di fatture o documenti attestanti operazioni inesistenti che precede, in una delle predette dichiarazioni siano indicati elementi attivi inferiori a quelli effettivi, oppure fittizi elementi passivi, crediti e ritenute, mediante la conclusione di operazioni simulate, oggettivamente o soggettivamente, oppure avvalendosi di documenti falsi, registrati nelle scritture contabili obbligatorie o conservati ai fini di prova, o di altri mezzi fraudolenti idonei a falsare la contabilità ostacolando l'accertamento o inducendo in errore l'Agenzia delle Entrate. Tale reato non sussiste quando non sono superate determinate soglie, oppure la falsa rappresentazione della realtà non sia ottenuto con artifici, ma si tratti di mera omissione degli obblighi di fatturazione e annotazione o della sola indicazione in dichiarazione di elementi attivi inferiori a quelli reali.

Entrambi i reati si perfezionano con la presentazione delle dichiarazioni. Sono però puniti anche i delitti tentati⁷⁷, ai sensi dell'art. 6 del D. Lgs. 74/2000, qualora siano compiuti atti preparatori della

⁷⁶ La disciplina dei reati tributari è stata riformata dal D. L. n. 124/2019, il cui articolo 39 ha introdotto nel D. Lgs. 231/2001 i reati tributari con effetto dal 24 dicembre 2019. L'articolo 5 del D. Lgs. n. 75/2020 vi ha poi aggiunto i reati di omessa o infedele dichiarazione e di indebita compensazione, ed ha reso punibili - modificando l'articolo 6 del D. Lgs. n.74/2000 - anche i reati dichiarativi di cui agli articoli 2, 3 e 4 solo tentati, con effetto dal 30 luglio 2020.

⁷⁷ Si ricorda che ai sensi dell'art. 26 del D. Lgs. 231/2001 la responsabilità degli enti per i delitti tentati non sussiste se l'ente volontariamente impedisce la finalizzazione dell'azione o il verificarsi dell'evento.

dichiarazione fraudolenta, che possano consistere ad esempio nella sola annotazione delle informazioni non veritiere nella contabilità, al fine di evadere l'IVA per un valore non inferiore a € 10 milioni e i fatti avvengano in parte in Italia e in parte in altro Stato dell'UE.

Dichiarazione infedele (art. 4 D. Lgs. 74/2000)

Omessa dichiarazione (art. 5 D. Lgs. 74/2000)

Indebita compensazione (art. 10-*quater* D. Lgs. 74/2000)

Tali reati puniscono rispettivamente chi:

- nelle dichiarazioni annuali dei redditi o IVA indica elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti, e siano superate determinate soglie di rilevanza penale;
- non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte (o la dichiarazione di sostituto di imposta) quando è superata una determinata soglia di imposta evasa;
- non versa le imposte dovute utilizzando in compensazione crediti non spettanti, per un importo annuo superiore a una determinata soglia.

Dette condotte comportano anche la responsabilità amministrativa ai sensi del D. Lgs. 231/2001 solo se hanno ad oggetto l'evasione dell'IVA per un importo non inferiore a € 10 milioni e se sono commesse nell'ambito di sistemi fraudolenti transfrontalieri.

In presenza di entrambe le circostanze il reato di dichiarazione infedele è punito, ai sensi dell'art. 6 del D. Lgs. 74/2000, anche se è solo tentato⁷⁸, quando cioè sussistano atti preparatori, quali ad esempio l'omissione di obblighi di fatturazione, che potranno quindi aver effetto sulla successiva dichiarazione, se tali fatti siano compiuti anche nel territorio di un altro Stato membro dell'UE.

Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D. Lgs. 74/2000)

Commette il reato chi, al fine di consentire a terzi l'evasione delle imposte sui redditi o l'IVA, emette o rilascia fatture o altri documenti per operazioni inesistenti.

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

Occultamento o distruzione di documenti contabili (art. 10 D. Lgs. 74/2000)

Il reato è commesso da chi, al fine di evadere le imposte sui redditi o l'IVA o di consentirne l'evasione da parte di terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti

⁷⁸ Cfr nota precedente

di cui è obbligatoria la conservazione, in modo da impedire la ricostruzione dei redditi o del volume d'affari.

Sottrazione fraudolenta al pagamento di imposte (art. 11 D. Lgs. 74/2000)

La condotta punita consiste nel compimento, sui beni propri o di terzi, di atti dispositivi simulati o fraudolenti, idonei a rendere incapiente la procedura di riscossione coattiva delle imposte sui redditi dell'IVA, di interessi o sanzioni amministrative relativi a tali imposte, per un ammontare complessivo superiore a 50 mila euro.

È altresì punita la condotta di chi nell'ambito di una procedura di transazione fiscale, al fine di ottenere per sé o per altri un minor pagamento di tributi e accessori, indica nella documentazione presentata elementi attivi inferiori a quelli reali o elementi passivi fittizi per un ammontare complessivo superiore a 50 mila euro.

7.10.2 Attività aziendali sensibili

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

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

- la Società ha aderito al regime del gruppo IVA di Intesa Sanpaolo S.p.A.⁷⁹. Al riguardo, la Capogruppo ha esercitato, con decorrenza 1° gennaio 2019, l'opzione per la costituzione di un Gruppo IVA così come disciplinato all'interno del Titolo V-bis del D.P.R. n. 633 e dal relativo decreto attuativo D.M. 6 aprile 2018. La partecipazione ad un Gruppo IVA comporta la nascita di un unico (nuovo) soggetto passivo, in quanto il Gruppo IVA: i) ha un'unica Partita IVA, ii) opera come soggetto passivo IVA unico nei rapporti con soggetti non appartenenti al gruppo stesso, iii) assolve tutti gli obblighi ed esercita tutti i diritti/opzioni (es. separazione delle attività ai fini IVA) rilevanti ai fini IVA. Il Gruppo IVA opera per il tramite della società rappresentante (Intesa Sanpaolo) che esercita il controllo sulle altre società partecipanti⁸⁰;
- con riferimento alle imposte sui redditi, la Società ha aderito al Consolidato Fiscale Nazionale⁸¹, disciplinato dagli artt. 117-129 del Testo Unico delle Imposte sul Reddito, che la Capogruppo Intesa Sanpaolo S.p.A. ha attivato, a partire dal 2004. Per effetto della citata opzione ogni società, continua a dichiarare autonomamente il proprio reddito o la propria perdita fiscale, oltre alle ritenute subite, alle detrazioni e ai crediti di imposta; tali componenti si intendono trasferite *ex lege* alla società controllante/consolidante che, nell'ambito della dichiarazione dei redditi

⁷⁹ A partire dal 1° gennaio 2023.

⁸⁰ La normativa prevede la partecipazione forzata (clausola "all-in all-out") di tutti i soggetti legati da vincoli finanziari, economici ed organizzativi con la Capogruppo.

⁸¹ A partire dall'anno d'imposta 2022.

consolidata (modello CNM) (i) determina un unico reddito imponibile o un'unica perdita fiscale riportabile risultante dalla somma algebrica di redditi/perdite propri e delle società consolidate, (ii) apporta le rettifiche di consolidamento previste dalla legge, (iii) scompota le ritenute e i crediti d'imposta propri e quelli trasferiti dalle consolidate per arrivare a determinare l'unico debito o credito IRES di competenza del Consolidato Fiscale.

Per quanto riguarda i rapporti con i terzi, quali fornitori, *partner* e controparti in genere al fine di mitigare il rischio di essere coinvolta in illeciti fiscali dei medesimi, la Società ha altresì predisposto i protocolli che disciplinano le seguenti attività:

- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
 - Gestione di omaggi, spese di rappresentanza e sponsorizzazioni;
 - Acquisto, gestione e cessione di partecipazioni e di altri *asset*;
 - Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose;
- che contengono principi di controllo e di comportamento da rispettare anche ai fini della prevenzione dei reati fiscali.

Detti protocolli si applicano anche a presidio delle attività svolte, sulla base di appositi contratti di servizio, dalla Capogruppo e/o *outsourcer* esterni.

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

Premessa

Il presente protocollo si applica a tutte le Unità Organizzative coinvolte nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari.

Le attività inerenti alla gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari sono svolte con il supporto delle strutture competenti della Capogruppo, anche in virtù di quanto previsto dal contratto di servizio in essere.

Ai sensi del D. Lgs. 231/2001, il processo potrebbe presentare occasioni per la commissione dei seguenti reati tributari: *“Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti”*, *“Dichiarazione fraudolenta mediante altri artifici”*, *“Emissione di fatture o altri documenti per operazioni inesistenti”*, *“Occultamento o distruzione di documenti contabili”* e di *“Sottrazione fraudolenta al pagamento di imposte”*, *“Dichiarazione infedele”*; *“Omessa dichiarazione”* e *“Indebita compensazione”*⁸².

Inoltre, le regole aziendali e i controlli di completezza e di veridicità previsti nel presente protocollo sono predisposti anche al fine di una più ampia azione preventiva dei reati che potrebbero conseguire a una scorretta gestione delle risorse finanziarie, quali i reati *“Riciclaggio”* e *“Autoriciclaggio”*.

Secondo quanto sancito dai *“Principi di condotta in materia fiscale”*, la Società, conformemente alla politica di Gruppo, intende mantenere un rapporto collaborativo e trasparente con l’Autorità Fiscale e promuovere l’adesione ai regimi di cooperative *compliance*.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Descrizione del processo

Il processo di gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari interessa, in modo diretto e/o indiretto, una serie eterogenea di processi aziendali che riguardano:

- le fasi di acquisto e di vendita di beni e servizi;
- la rappresentazione dei fatti di gestione nella contabilità e nei sistemi aziendali;
- la gestione degli adempimenti connessi alla fatturazione attiva e passiva e di quelli relativi al *“Gruppo IVA”*;
- la predisposizione delle dichiarazioni fiscali e la corretta liquidazione/riversamento delle relative imposte;

⁸² La possibilità di commissione dei reati di *“Dichiarazione infedele”*, *“Omessa dichiarazione”* e *“Indebita compensazione”*, tenuto conto dell’operatività della Società, è da ritenersi ragionevolmente remota.

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

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

Le modalità operative per la gestione del processo sono disciplinate nell’ambito della normativa interna e/o di Gruppo applicabile, sviluppata ed aggiornata a cura delle Unità Organizzative, che costituisce parte integrante e sostanziale del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti nell’ambito del processo:
 - tutti i soggetti che intervengono nella gestione delle attività inerenti alla predisposizione delle dichiarazioni fiscali, e nelle prodromiche attività di emissione/contabilizzazione delle fatture: sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal Responsabile della struttura di riferimento tramite delega interna, da conservare a cura della Struttura medesima;
 - nel caso in cui intervengano consulenti esterni/fornitori, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali; operano esclusivamente nell’ambito del perimetro di attività loro assegnato dal Responsabile della struttura di riferimento;
 - ogni accordo/convenzione con l’Agenzia delle Entrate è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere.
- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi di gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari. In particolare:
 - le attività di cui alle diverse fasi del processo devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.
- Attività di controllo:
 - controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle autorità fiscali da parte della Struttura interessata per le attività di competenza che devono essere supportate da meccanismi di maker e checker;
 - controlli di carattere giuridico sulla conformità alla normativa di riferimento della dichiarazione fiscale;
 - controlli continuativi automatici di sistema, con riferimento alle dichiarazioni periodiche;

- controlli sulla corretta emissione, applicazione delle aliquote IVA e contabilizzazione delle fatture del ciclo attivo e sulla loro corrispondenza con i contratti e impegni posti in essere con i terzi;
- controlli sull'effettività, sia dal punto di vista soggettivo che oggettivo, del rapporto sottostante alle fatture passive ricevute e sulla corretta registrazione e contabilizzazione.
- Tracciabilità del processo sia a livello di sistema informativo, sia in termini documentali:
 - ciascuna fase rilevante del processo di gestione del rischio e degli adempimenti ai fini della prevenzione dei reati tributari deve risultare da apposita documentazione scritta;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.
- Sistemi premianti o di incentivazione: i sistemi premianti e di incentivazione devono essere in grado di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Principi di comportamento

Le Strutture della Società, a qualsiasi titolo coinvolte nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari oggetto del protocollo, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico, del Codice Interno di Comportamento di Gruppo, e dei Principi di condotta in materia fiscale. In particolare, tutte le Strutture sono tenute – nei rispettivi ambiti - a:

- garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari della Società nelle dichiarazioni fiscali;
- rispettare i principi di condotta in materia fiscale al fine di: (i) garantire nel tempo la conformità alle regole fiscali e tributarie dei Paesi dove la Società opera e, (ii) l'integrità patrimoniale e la reputazione di tutte le Società Gruppo;
- agire secondo i valori dell'onestà e dell'integrità nella gestione della variabile fiscale, nella consapevolezza che il gettito derivante dai tributi costituisce una delle principali fonti di contribuzione allo sviluppo economico e sociale dei Paesi in cui opera;
- garantire la diffusione di una cultura aziendale improntata ai valori di onestà e integrità e al principio di legalità;
- mantenere un rapporto collaborativo e trasparente con l'Autorità Fiscale garantendo a quest'ultima, tra l'altro, la piena comprensione dei fatti sottesi all'applicazione delle norme fiscali;

- eseguire gli adempimenti fiscali nei tempi e nei modi definiti dalla normativa o dall'autorità fiscale;
- evitare forme di pianificazione fiscale che possano essere giudicate aggressive da parte delle autorità fiscali;
- interpretare le norme in modo conforme al loro spirito e al loro scopo rifuggendo da strumentalizzazioni della loro formulazione letterale;
- rappresentare gli atti, i fatti e i negozi intrapresi in modo da rendere applicabili forme di imposizione fiscale conformi alla reale sostanza economica delle operazioni;
- garantire trasparenza alla propria operatività e alla determinazione dei propri redditi e patrimoni evitando l'utilizzo di strutture, anche di natura societaria, che possano occultare l'effettivo beneficiario dei flussi reddituali o il detentore finale dei beni;
- rispettare le disposizioni atte a garantire idonei prezzi di trasferimento per le operazioni infragruppo con la finalità di allocare, in modo conforme alla legge, i redditi generati;
- collaborare con le autorità competenti per fornire in modo veritiero e completo le informazioni necessarie per l'adempimento e il controllo degli obblighi fiscali;
- stabilire rapporti di cooperazione con le amministrazioni fiscali, ispirati alla trasparenza e fiducia reciproca e volti a prevenire i conflitti, riducendo quindi la possibilità di controversie;
- proporre alla clientela servizi che non consentano di conseguire indebiti vantaggi fiscali non altrimenti ottenibili, prevedendo inoltre idonee forme di presidio per evitare il coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela.

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

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

obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento; iii) una base imponibile in misura inferiore a quella effettiva attraverso l'esposizione di elementi attivi per un ammontare inferiore a quello reale o di elementi passivi fittizi; iv) fare decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle medesime così come per il successivo versamento delle imposte da esse risultanti.

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