SOMMARIVA 14 S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

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

Approvato dal Consiglio di Amministrazione del 18/09/2025

INDICE

Capitolo 1 – Il contesto normativo

1.1 Il regime di responsabilità amministrativa previsto dal Decreto Legislativo n. 231/2001 a carico delle persone giuridiche, società ed associazioni

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. n. 231/2001"), 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 commessi[1] 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.

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.

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 dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, "*modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi*".

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

Il modello di organizzazione, gestione e controllo (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 a 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 eserci-

[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.

tano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che: (i) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi; (ii) 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; (iii) i soggetti hanno commesso il reato eludendo fraudolentemente il Modello; (iv) 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 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.

Capitolo 2 - Il Modello di organizzazione, gestione e controllo di Sommariva 14 S.r.l.

2.1 Premessa

Sommariva 14 S.r.l. (di seguito anche "Sommariva" o la "Società") ha per oggetto le seguenti attività: l'acquisto e vendita di terreni e/o fabbricati, nonché la costruzione e/o ristrutturazione, nell'ambito di aree in proprietà, di fabbricati, la loro conduzione, locazione, gestione e vendita.

La Società è controllata al 100% dal Fondo Pensione a Prestazione definita del Gruppo Intesa Sanpaolo (di seguito anche il "Fondo" o il "Controllante") a seguito dell'efficacia delle disposizioni di cui all'Accordo Collettivo sottoscritto dalle Fonti Istitutive (in data 5 dicembre 2017) riguardante la razionalizzazione della previdenza integrativa del Gruppo Intesa Sanpaolo, con cui si è realizzata - con effetto dall'1/1/2019 - l'integrazione della Cassa di Previdenza Integrativa per il Personale dell'Istituto Bancario Sanpaolo di Torino (precedente Socio unico della Società) nel suddetto Fondo.

L'assetto organizzativo della Società ha caratteri peculiari: le attività operative sono, infatti, concretamente gestite da specifiche risorse all'uopo rese disponibili da Intesa Sanpaolo S.p.A. (distaccate presso il Fondo controllante e operanti anche presso la Società) ovvero delegate a soggetti esterni specializzati nei rispettivi campi, sulla base di specifici contratti.

2.2 Gli strumenti esistenti quali presupposti del Modello

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

Il contesto organizzativo della Società è costituito dall'insieme di regole, strutture e procedure che garantiscono il funzionamento della Società stessa.

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

- le procedure interne (della Società e/o del Controllante);
- il Codice Etico del Controllante (di seguito anche "Codice Etico"), ai cui principi la Società si attiene;
- 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 successivi paragrafi sono illustrati, per grandi linee, esclusivamente i principi di riferimento del Codice Etico, il sistema dei controlli interni, nonché il sistema dei poteri e delle deleghe.

2.1.1 Codice Etico

A conferma dell'importanza attribuita ai profili etici, la Società si attiene ai principi contenuti nel Codice Etico del Controllante, che integrano quelli contenuti nel presente Modello.

Il Codice Etico riveste una portata generale, in quanto contiene una serie di principi deontologici che la Società riconosce come propri e sui quali intende richiamare l'osservanza di tutti coloro che, all'interno della stessa, cooperano al perseguimento dei fini istituzionali.

Si rammenta che il personale distaccato dalla Banca che opera presso il Fondo controllante e presso la Società è anche tenuto – nell'ambito del rapporto di lavoro – al rispetto dei valori e dei principi del Codice Etico adottato da Intesa Sanpaolo S.p.A.

2.2.2 Le caratteristiche salienti del sistema dei controlli interni

Il sistema dei controlli interni della Società si basa principalmente sull'insieme di regole, procedure e strutture organizzative adottate dalla Società stessa, che mirano ad assicurare il conseguimento delle seguenti finalità:

- efficacia ed efficienza dei processi operativi;
- salvaguardia del valore delle attività e protezione dalle perdite;
- affidabilità e integrità delle informazioni contabili e gestionali;
- conformità delle operazioni con la legge, nonché con la normativa interna.

L'impianto normativo è costituito da "Documenti di Governance" che sovraintendono al funzionamento della Società (Codice Etico, Deleghe e poteri, ecc.) e da norme più strettamente operative che regolamentano alcuni processi della Società, le singole attività e i relativi controlli (procedure operative della Società e/o del Controllante).

Più nello specifico le regole operative adottate disegnano soluzioni organizzative che:

- assicurano una sufficiente separatezza tra le funzioni operative e quelle di controllo ed evitano situazioni di conflitto di interesse nell'assegnazione delle competenze;
- sono in grado di identificare, misurare e monitorare adeguatamente i principali rischi assunti nei diversi segmenti operativi;
- consentono la registrazione di ogni fatto di gestione e, in particolare, di ogni operazione con adeguato grado di dettaglio, assicurandone la corretta attribuzione sotto il profilo temporale;
- assicurano sistemi informativi affidabili e idonee procedure di reporting ai diversi livelli direzionali ai quali sono attribuite funzioni di controllo;
- garantiscono che le anomalie riscontrate dai singoli soggetti, dalla Funzione Revisione Interna - Internal Audit del Controllante o da altri addetti ai controlli siano tempestivamente portate a conoscenza di livelli appropriati della Società e gestite con immediatezza.

Inoltre, le soluzioni organizzative adottate dalla Società prevedono attività di controllo che consentano 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 della Società e al contesto di riferimento.
I controlli coinvolgono, con ruoli diversi, il Consiglio di Amministrazione, il Collegio dei Sindaci, il Direttore Operativo della Società, l'Internal Audit del Controllante, tutto il personale dipendente della Banca che opera in nome e per conto della Società (di seguito anche "personale"), e rappresentano un attributo imprescindibile dell'attività quotidiana della Società stessa.

2.2.3 Il sistema dei poteri e delle deleghe

A norma di Statuto, il Consiglio di Amministrazione è investito di tutti i poteri di ordinaria e straordinaria amministrazione e di disposizione - ivi compresi quelli di consentire iscrizioni, surroghe, postergazioni e cancellazioni di ipoteche e privilegi, sia totali che parziali, nonché di fare e cancellare trascrizioni ed annotamenti di qualsiasi specie, anche indipendentemente dal pagamento dei crediti ai quali dette iscrizioni, trascrizioni ed annotamenti si riferiscono – escluso soltanto quanto la legge riserva all'esclusiva competenza dei soci.

Il Consiglio ha conferito al Presidente del Consiglio di Amministrazione della società i necessari poteri per le attività di ordinaria amministrazione.

Il Consiglio di Amministrazione ha inoltre nominato il Direttore Operativo cui è attribuita procura speciale affinché possa compiere per la Società atti necessari per lo svolgimento di alcuni atti di gestione sociale, con particolare riguardo agli aspetti della quotidiana gestione aziendale.

Il Direttore Operativo è individuato anche quale Datore di lavoro e Committente ai sensi del D.Lgs. n. 81/2008, oltre agli specifici compiti attribuitigli dalla procura speciale, ha altresì la responsabilità di presidiare la struttura organizzativa al fine di garantire l'efficace operatività della Società.
Il Consiglio di Amministrazione ha inoltre attribuito una procura per la vendita frazionata delle unità immobiliari residuali di proprietà della società mandante.

Il Direttore Generale del Fondo controllante (Socio unico della Sommariva 14 Srl) viene individuato anche quale Direttore Operativo della controllata Sommariva 14 Srl e per essa le Strutture del Fondo svolgono le attività competenti, ove applicabili. Nell'adunanza del 27 giugno 2023 il Consiglio di Amministrazione del Fondo ha confermato al Direttore Generale anche le nomie di Referente privacy, Responsabile in materia di salute e sicurezza sui luoghi di lavoro ai sensi del D.Lgs. n. 81/2008 e di Delegato in materia ambientale ai sensi del D.Lgs. n. 152/2006.

2.3 Le finalità perseguite con l'adozione del Modello

Nonostante gli strumenti a supporto dell'operatività utilizzati ed illustrati nei paragrafi precedenti risultino di per sé idonei anche a prevenire i reati contemplati dal Decreto, la Società ha ritenuto opportuno adottare uno specifico Modello di organizzazione, gestione e controllo ai sensi del Decreto, 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 intende attenersi nell'esercizio della propria attività;
- 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.

2.4 Gli elementi fondamentali del Modello

Il Modello della Società è stato predisposto in coerenza con la volontà del Legislatore, tenuto conto dei criteri e delle linee guida utilizzati dal proprio Controllante e dalla Banca nella redazione dei rispettivi Modelli nonchè dell'informativa disposta in materia dalle associazioni di categoria.
Gli elementi fondamentali sviluppati nella definizione del Modello possono essere così brevemente riassunti:

- individuazione delle aree di attività a rischio ovvero delle attività 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;

- corrette modalità di svolgimento delle attività e il corretto funzionamento dei sistemi informatici a loro supporto comprese quelli basati su tecniche di intelligenza artificiale;
- la tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali o informatici;
- processi decisionali legati a predefiniti criteri oggettivi;
- l'esistenza e la tracciabilità delle attività di controllo e supervisione sulle diverse operazioni compiute;
- la presenza di meccanismi di sicurezza in grado di assicurare un'adeguata protezione/accesso fisico-logico ai dati e ai beni della Società;

- emanazione di regole comportamentali idonee a garantire l'esercizio delle attività nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio della Società;
- 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 del personale e comunicazione interna in merito al contenuto del Decreto e del Modello ed agli obblighi che ne conseguono.

2.5 La Struttura del Modello

Nel definire il presente "Modello di organizzazione, gestione e controllo" la Società ha adottato un approccio che ha consentito di utilizzare ed integrare nel Modello stesso le regole e la normativa interna esistenti, sulla base della mappatura delle aree e attività sensibili effettuata tramite specifici incontri con il personale della Società maggiormente coinvolto nelle aree a rischio. Sono state così identificate per ciascuna categoria di "illeciti presupposto", le aree di attività "sensibili". Nell'ambito di ogni area sensibile sono state poi individuate le attività 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.

Si precisa che la mappatura delle aree e attività sensibili alla base della predisposizione e dei successivi aggiornamenti del presente Modello è stata condotta in considerazione di tutte le fattispecie di reato previste dal D.Lgs. 231/2001 alla data di ultimo aggiornamento del Modello. A tal proposito si evidenzia che il mancato richiamo, nel Modello stesso, di determinate fattispecie contemplate nel Decreto e/o l'assenza di appositi principi di controllo e di comportamento a presidio del rischio di commissione delle stesse, consegue all'identificazione di un connesso livello di rischio-reato pressoché nullo o molto contenuto.

All'interno della Società il presidio dei rischi rivenienti dal D.Lgs. n. 231/2001 è pertanto assicurato:

- dal presente documento ("Modello di organizzazione, gestione e controllo"), e
- dall'impianto normativo esistente, che ne costituisce parte integrante.

Il "Modello di organizzazione, gestione e controllo" delinea in particolare:

- il contesto normativo di riferimento;
- il ruolo e la responsabilità 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 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 di Sommariva regolamenta ai vari livelli l’operatività della Società nelle aree/attività “sensibili” e costituisce a tutti gli effetti parte integrante del Modello. Tale impianto è diffuso all’interno di tutta la Società tramite la rete Intranet e l’area condivisa sul server del Fondo, costantemente aggiornate a cura dei soggetti competenti in coerenza con l’evolversi dell’operatività.

2.6 I destinatari del Modello

Il Modello e le disposizioni ivi contenute e richiamate devono essere rispettate dagli esponenti della Società e da tutti il personale della Società (per personale” deve intendersi: “i dipendenti distaccati dalla Banca che operano presso il Fondo controllante e la Società stessa, e coloro che comunque operano sulla base di rapporti che ne determinano l’inserimento nell’organizzazione della Società, anche in forma diversa dal rapporto di lavoro subordinato”) e, in particolare, da parte di coloro che si trovino a svolgere le attività sensibili.
La formazione 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, i fornitori) 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 ed a segnalare all’Organismo di Vigilanza eventuali notizie della commissione di illeciti o della violazione del Modello, prevedendosi che la violazione degli impegni o, comunque, 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.
In relazione ai dipendenti di Intesa Sanpaolo S.p.A. che, a vario titolo, operano in nome e per conto della Società, si sottolinea come questi siano comunque destinatari diretti anche del Modello ex D.Lgs. 231/2001 predisposto dalla Banca stessa.

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

Adozione del Modello

L’adozione e l’efficace attuazione del Modello 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 stesso.

Il Direttore Operativo della Società presidia la struttura del Modello da sottoporre all’approvazione del Consiglio di Amministrazione con il supporto dell’Organismo di Vigilanza e della struttura Legale – Rapporti con Iscritti e Processi Operativi del Controllante.

Efficace attuazione e modificazione del Modello

E’ 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, il Consiglio di Amministrazione si avvale del supporto dell’Organismo di Vigilanza.
Il Consiglio di Amministrazione delega i singoli soggetti a dare attuazione ai contenuti del Modello ed a curare il costante aggiornamento e implementazione della normativa interna e dei processi operativi, che costituiscono parte integrante del Modello, nel rispetto dei principi di controllo e di comportamento definiti in relazione ad ogni attività sen-

sibile. Delle modifiche intervenute nei processi e nella normativa interna in questione verrà data idonea informativa al Consiglio di Amministrazione e all'Organismo di Vigilanza.

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 dai singoli soggetti nelle aree sensibili;
- dai singoli soggetti coinvolti in relazione alle attività a rischio dagli stessi svolti.

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 rendessero necessarie nel futuro.

Specifici ruoli e responsabilità nella gestione del Modello sono inoltre attribuiti alle funzioni e ai soggetti della Società e del Controllante ovvero alle strutture della Banca di seguito indicati.

Funzione Revisione Interna - Internal Audit

La Funzione Revisione Interna - Internal Audit del Controllante (di seguito "Internal Audit") riferisce direttamente al Consiglio di Amministrazione garantendo l'indipendenza, l'autonomia e l'obiettività di giudizio della propria attività.

Tale struttura garantisce un adeguato presidio circa l'imparzialità dell'operato, la qualità, l'indipendenza e l'obiettività di giudizio della Funzione e dei suoi componenti.

Alla Funzione sono assegnati i seguenti compiti:

- valutare e monitorare l'efficacia, l'efficienza e l'adeguatezza del sistema di controllo interno e delle ulteriori componenti del sistema di governo del Fondo, nonché l'efficacia e l'efficienza delle attività esternalizzate, inclusa l'efficacia dei controlli svolti su tali attività;
- verificare la correttezza dei processi interni e l'efficacia e l'efficienza delle procedure organizzative, nonché la regolarità e la funzionalità dei flussi informativi tra i diversi settori del Fondo;
- presidiare l'adeguatezza dei sistemi informativi e la loro affidabilità, affinché non sia inficiata la qualità delle informazioni, nonché la rispondenza delle rilevazioni e dei processi amministrativi contabili e gestionali a criteri di correttezza e di regolare tenuta della contabilità;
- formulare raccomandazioni al Consiglio di Amministrazione e controllare l'avvenuta rimozione delle anomalie riscontrate nell'operatività del fondo e nel funzionamento dei controlli interni (attività cosiddetta di follow-up);
- comunicare all'Autorità di Vigilanza le situazioni problematiche riscontrate nello svolgimento della propria attività qualora le stesse non abbiano trovato, come dovrebbero, soluzione all'interno del Fondo;
- collaborare alla redazione ed aggiornamento della normativa interna;
- fornire un'attività di supporto consultivo alle strutture operative con riferimento a specifici argomenti, al funzionamento dei processi ed all'evoluzione della normativa;
- collaborare con l'Organismo di Vigilanza ex-D.Lgs.231/01 nell'attività di presidio dell'adeguatezza ed efficacia del Modello di organizzazione, gestione e controllo;
- presentare al Consiglio di Amministrazione il Piano annuale dei controlli e semestralmente una relazione sull'attività svolta;
- svolgere l'incarico di Responsabile delle Segnalazioni Whistleblowing (cfr. Sezione "Whistleblowing").

Inoltre, la Funzione Revisione Interna - Internal Audit provvede a presidiare l'adeguatezza dei sistemi informativi e la loro affidabilità, assicura 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 rschiose, valutando la funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi operativi.

L'Internal Audit vigila sul rispetto e sull'adeguatezza delle regole delle procedure, attivando, a fronte delle eventuali criticità riscontrate nel corso della propria attività, i soggetti di volta in volta competenti per le opportune azioni di mitigazione, informando il Consiglio di Amministrazione e l'Organismo di Vigilanza in relazione a qualsiasi fattispecie rilevata che possa integrare una violazione del Modello o una carenza idonea a costituire i presupposti per una violazione.

L'Internal Audit supporta inoltre l'Organo di Vigilanza nello svolgimento delle sue attività di controllo mediante suggerimenti per l'aggiornamento del Modello, congiuntamente con il Legale – Rapporti con gli Iscritti e Processi Operativi del Controllante, in coerenza con l'evoluzione della normativa di riferimento e con le modifiche della struttura organizzativa della Società.

Legale – Rapporti con gli Iscritti e Processi Operativi

La struttura Legale – Rapporti con gli Iscritti e Processi Operativi del Controllante (di seguito "Legale"), per il perseguimento delle finalità di cui al Decreto, assicura assistenza e consulenza legale a tutto il personale della controllante nello svolgimento delle relative attività della Società, seguendo l'evolversi della normativa specifica e degli orientamenti giurisprudenziali in materia.

Spetta altresì al Legale l'interpretazione della normativa, la risoluzione di questioni di diritto e l'identificazione delle condotte che possono configurare ipotesi di reato.

Legale collabora con l'Internal Audit all'adeguamento del Modello, segnalando anche eventuali estensioni dell'ambito di responsabilità amministrativa degli Enti.

In particolare, la Struttura svolge le seguenti attività:

- gestione delle richieste di convocazioni delle Direzioni Provinciali del Lavoro, Organismi di mediazione, delle richieste di informazioni della Guardia di Finanza o di altri Enti della P.A.;
- gestione delle vertenze giudiziali;
- esercizio della procura speciale di rappresentanza processuale per intervenire in udienze o presso organismi di conciliazione, rilasciare o sottoscrivere atti, verbali o dichiarazioni, anche in qualità di terzo pignorato o sequestrato;
- supporto al Direttore Generale ed al Vice Direttore dell'Area Operativa e Compliance nella scelta del professionista da incaricare per la difesa del Fondo, curando i rapporti con il professionista per la gestione dell'istruttoria e riscontrando, anche in corso di giudizio, le eventuali ulteriori richieste dello stesso;
- gestione delle attività inerenti alle Segnalazioni di Vigilanza per gli aspetti di competenza;
- gestione dei Reclami;
- gestione dei rapporti con i consulenti normativi e fiscali interni ed esterni al Gruppo;
- gestione del processo di zainettizzazione della prestazione definita e supporto agli iscritti per tale attività;
- collaborazione con le altre strutture e supporto del Service Previdenziale nella corretta gestione delle attività inerenti alle prestazioni pensionistiche, coordinando le attività da intraprendere con le competenti strutture della Banca;
- presidio dell'operato delle attività esternalizzate per gli aspetti di competenza;
- predisposizione di note alla COVIP a seguito di disposizioni normative relative all'ambito di competenza;
- predisposizione delle pratiche per il Consiglio di Amministrazione per gli aspetti di competenza;
- supporto al Vice Direttore dell'Area Operativa e Compliance per presidiare la compliance del Fondo ed in particolare il rischio di non conformità nelle sue componenti di rischio legale e rischio reputazionale, al fine di prevenire la violazione di norme e di regole e procedure deliberate dall'organo di amministrazione, di evitare il rischio di incorrere in sanzioni, perdite finanziarie o danni di reputazione in conseguenza di violazioni di norme legislative, regolamentari o di autoregolamentazione.

Funzioni Tutela Aziendale, Ambiente ed Energia (Intesa Sanpaolo)

Per il perseguimento delle finalità di cui al D. lgs. 231/2001 le funzioni Tutela Aziendale, Ambiente ed Energia di Intesa Sanpaolo limitatamente alla gestione dei rischi in materia di salute e sicurezza e per l'ambiente:

- partecipano alla definizione della struttura del Modello e all'aggiornamento dello stesso;
- verificano nel continuo che le procedure aziendali siano coerenti con gli adempimenti previsti dalla normativa e le politiche aziendali e ne promuovono le modifiche finalizzate ad assicurare un adeguato presidio del rischio di non conformità con riferimento agli ambiti di Tutela della Salute e della Sicurezza sul Lavoro, ai sensi del D.Lgs. 81/2008 e Tutela Ambientale, ai sensi del D.Lgs. 152/2006;
- definiscono e attuano piani di verifiche periodiche per garantire il presidio del rischio di non conformità;
- curano, in raccordo con le altre funzioni aziendali competenti in materia di formazione, la predisposizione di adeguate attività formative, finalizzate a conseguire un aggiornamento su base continuativa dei dipendenti e dei collaboratori.

Funzione Personale (Intesa Sanpaolo)

Con riferimento al Decreto, la Funzione Personale di Intesa Sanpaolo, come in dettaglio illustrato al Capitolo 5 ed al Capitolo 6:

- programma piani di formazione e interventi di sensibilizzazione rivolti a tutti i dipendenti della Banca che operano in nome e per conto della Società sull'importanza di un comportamento conforme alle regole definite, sulla comprensione dei contenuti del Modello, del Codice Etico, nonché specifici corsi destinati al personale che opera nelle aree sensibili identificate all'interno della Società, 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 dell'Internal Audit e del Legale, il processo di rilevazione e gestione delle violazioni del Modello, e attiva su proposta del Consiglio di Amministrazione il conseguente processo sanzionatorio; fornisce inoltre 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, il quale le analizza al fine di prevenire future violazioni, nonché di monitorare l'adeguatezza del Modello.

Direttore Operativo

Il Direttore Operativo della Società, oltre agli specifici compiti attribuitigli dalla Procura speciale, al fine di meglio presidiare la coerenza della struttura organizzativa e dei meccanismi di governance rispetto agli obiettivi perseguiti con il Modello, ha la responsabilità di:

- definire la struttura organizzativa, definendone missioni, organigrammi e funzioni, al fine di sottoporla all'approvazione del Consiglio di Amministrazione;
- collaborare con l'Internal Audit e il Legale e con gli altri soggetti interessati, ognuno 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).

Il Direttore Operativo è stato individuato come Datore di lavoro e Committente ai sensi del D.Lgs. n. 81/2008. Come tale, in relazione alla gestione dei rischi in materia di salute sicurezza nei luoghi di lavoro:

- partecipa alla definizione della struttura del Modello ed all'aggiornamento dello stesso;
- individua e valuta l'insorgenza di fattori di rischio dai quali possano derivare la commissioni di illeciti presupposto;
- promuove le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio di non conformità.

Personale della Società

Al personale della controllante nello svolgimento delle attività della Società, è assegnata la responsabilità dell'esecuzione, del buon funzionamento e della efficace applicazione nel tempo dei processi.

Agli specifici fini del Decreto, il personale della Società ha 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, il personale della controllante coinvolto nelle attività sensibili, deve 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.

2.8 Attività oggetto di outsourcing

Il modello organizzativo della Società prevede l'esternalizzazione (di seguito anche "outsourcing") di attività, o parti di esse, presso la Banca, altre Società del Gruppo Intesa Sanpaolo o altre Società terze.

L'affidamento in outsourcing delle attività è realizzato in conformità alle prescrizioni delle competenti Autorità di Vigilanza ed è formalizzato attraverso la stipula di specifici contratti che consentono alla Società:

- di assumere ogni decisione nell'esercizio della propria autonomia, conservando le necessarie competenze e responsabilità sulle attività relative ai servizi esternalizzati;
- di mantenere conseguentemente i poteri di indirizzo e controllo sulle attività esternalizzate.

I contratti di outsourcing devono prevedere che:

- l'attività esternalizzata, le modalità di esecuzione e il relativo corrispettivo siano definite chiaramente;
- il fornitore svolga adeguatamente l'esecuzione delle attività esternalizzate nel rispetto della normativa vigente e delle disposizioni della Società;
- il fornitore informi tempestivamente la Società di qualsiasi fatto che possa incidere in maniera rilevante sulla propria capacità di eseguire le attività esternalizzate in conformità alla normativa vigente e in maniera efficiente ed efficace;
- il fornitore garantisca la riservatezza dei dati relativi alla Società;
- la Società abbia, tramite apposite strutture, facoltà di controllo degli eventuali SLA (Service Level Agreement) e del rispetto delle clausole contrattuali e accesso all'attività e alla documentazione del fornitore;
- il fornitore garantisca l'accesso completo ed immediato alle Autorità di Controllo ai locali e alla documentazione richiesta;
- la Società possa recedere dal contratto senza oneri sproporzionati o tali da pregiudicare, in concreto, l'esercizio del diritto di recesso;
- la Società possa risolvere il contratto in caso di violazione da parte dell'outsourcer di norme e regolamenti di vigilanza che comportino sanzioni a carico del committente o violazioni di quanto previsto all'interno del Modello e del Codice Etico;
- il contratto non possa essere oggetto di subcessione senza il consenso della Società;
- siano adottati adeguati presidi a tutela del patrimonio informativo della Società e della sicurezza delle transazioni.

2.9 Principi di indirizzo del Controllante in materia di Responsabilità amministrativa

Ferma restando l'autonoma responsabilità di Sommariva in ordine all'adozione ed all'efficace attuazione di un proprio Modello ai sensi del Decreto, il Fondo, nell'esercizio della sua peculiare funzione di Controllante, ha il potere di impartire criteri e direttive di carattere generale e di verificarne la rispondenza nel Modello adottato.

In particolare, la Società deve:

- adottare il proprio Modello, dopo aver individuato le attività operative che presentano un rischio di commissione degli illeciti previsti dal Decreto e le misure più idonee a prevenirne la realizzazione. Nella predisposizione del Modello la Società deve attenersi ai principi e ai contenuti del Modello del Controllante, salvo che sussistano situazioni specifiche relative alla natura, dimensione o al tipo di attività esercitata nonché alla struttura interna,

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;

- provvedere tempestivamente alla nomina dell'Organismo di Vigilanza, in linea con le indicazioni fornite dal Controllante in relazione ai soggetti da nominare;
- 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;
- predisporre, coordinandosi con le competenti funzioni del Fondo, piani di formazione e di comunicazione rivolti indistintamente a tutto il Personale con l'obiettivo di creare una conoscenza diffusa e una adeguata cultura aziendale 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.

Con riferimento alle attività sopra illustrate i competenti soggetti del Fondo forniscono a Sommariva supporto e collaborazione, per quanto di rispettiva competenza, nell'espletamento dei compiti alle stesse spettanti.

Capitolo 3 - L'Organismo di Vigilanza

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").

Le attribuzioni ed i poteri dell'Organismo di Vigilanza (di seguito, anche l'"Organismo") sono conferiti ad un organo collegiale nominato dal Consiglio di Amministrazione e avente 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 è data formale comunicazione a tutto il personale della Società.

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.

Il funzionamento dell'Organismo di Vigilanza è disciplinato da un apposito Regolamento, approvato dal medesimo.

L'Organismo di Vigilanza si avvale ordinariamente delle funzioni della Società e del Fondo Controllante per l'espletamento dei suoi compiti di vigilanza e controllo ed *in primis* dell'Internal Audit, funzione istituzionalmente dotata di competenze tecniche e risorse, umane e operative, idonee a garantire lo svolgimento su base continuativa delle verifiche, delle analisi e degli altri adempimenti necessari. Laddove ne ravvisi la necessità, in funzione della specificità degli argomenti trattati, può inoltre avvalersi di consulenti esterni.

Per quanto concerne in particolare la materia della tutela della salute e della sicurezza sui luoghi di lavoro, l'Organismo potrà avvalersi anche di tutte le risorse[2] attivate per la gestione dei relativi aspetti (Responsabile del Servizio Prevenzione e Protezione, Rappresentante dei Lavoratori per la Sicurezza, Medico Competente, ecc.), nonché di quelle ulteriori previste dalle normative di settore e, in particolare, dal D.Lgs. n. 81/2008.

L'Organismo di Vigilanza, direttamente o per il tramite delle varie funzioni all'uopo designate, ha accesso a tutte le attività svolte dalla Società nelle aree a rischio e alla relativa documentazione.

3.2 Composizione, durata e compensi dell'Organismo di Vigilanza

3.2.1 Composizione

L'Organismo di Vigilanza è composto da tre membri effettivi, nominati dal Consiglio di Amministrazione della Società, fra i quali:

- un Sindaco effettivo
- un membro del Consiglio di Amministrazione
- un membro facente capo alla struttura della Funzione Revisione Interna – Internal Audit del Fondo.

L'Organismo nomina al proprio interno il Presidente tenendo conto degli eventuali orientamenti all'uopo forniti dal Consiglio di Amministrazione della Società all'atto della nomina.

[2] Si fa riferimento a risorse di Intesa Sanpaolo S.p.A. (fatta eccezione per il Datore di Lavoro ex D.Lgs. 81/08, nominato nell'ambito della Società, come sopra esposto). Infatti, come meglio specificato nel capitolo 7.7 "Area sensibile concernente i reati in tema di salute e sicurezza sul lavoro", Intesa Sanpaolo S.p.A. presta specifici servizi a favore della Società ai fini del rispetto degli adempimenti previsti dalle disposizioni normative vigenti in materia di salute e sicurezza nei luoghi di lavoro (D.Lgs. 81/08).

Al fine di assicurare l'operatività dell'Organismo di Vigilanza anche nei casi di sospensione ovvero di temporaneo impedimento di un componente, il Consiglio di Amministrazione nomina altresì un componente supplente che subentra al componente effettivo che si venga a trovare in una delle predette situazioni.

3.2.2 Durata

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 di Vigilanza dura in carica per tutto il periodo in cui resta in carica il Consiglio di Amministrazione che lo ha nominato. La revoca dei componenti - fatti salvi i casi disciplinati nel presente capitolo 3 - può avvenire unicamente nel caso di rilevanti inadempimenti nell'assolvimento dei loro compiti.

L'Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o decadenza, la maggioranza dei componenti. In tal caso il Consiglio di Amministrazione provvede tempestivamente a nominare i nuovi membri.

3.2.3 Compensi

Il Consiglio di Amministrazione delibera l'eventuale compenso spettante ai componenti dell'Organismo di Vigilanza per lo svolgimento delle relative funzioni, stabilendo altresì l'eventuale compenso spettante al membro supplente dell'Organismo stesso, anche sotto forma di emolumento fisso in ragione della sua partecipazione alle riunioni.

Ai membri – effettivi e supplente – compete altresì il rimborso delle spese vive e documentate sostenute per intervenire alle riunioni.

L'attività svolta dai componenti dell'Organismo di Vigilanza individuati fra i dipendenti della Banca è considerata attività di servizio a tutti gli effetti.

3.3 Requisiti di eleggibilità; cause di decadenza e sospensione; temporaneo impedimento

3.3.1 Requisiti di professionalità, onorabilità ed indipendenza

I membri dell'Organismo di Vigilanza dovranno possedere i requisiti di professionalità previsti per i soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le forme pensionistiche complementari (D.M. 11 giugno 2020 n. 108). Tutti i membri dell'Organismo dovranno inoltre possedere i requisiti di onorabilità secondo la normativa tempo per tempo vigente.

I componenti dell'Organismo di Vigilanza, che ricoprono anche il ruolo di membro del Collegio dei Sindaci, devono possedere i requisiti di indipendenza di cui all'art. 2399 del Codice Civile.

In aggiunta al possesso dei requisiti sopra richiamati i membri effettivi e il membro supplente dovranno 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, fatti salvi gli effetti della riabilitazione, per uno dei seguenti reati: reati per i quali è applicabile il D.Lgs. n. 231/2001; reati in materia di crisi d'impresa e di insolvenza[3]; delitti fiscali.
- abbiano rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società o ente nei cui confronti siano state applicate, con provvedimento definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
- si trovino in una delle condizioni di cui all'art.2382 c.c.
- si trovino in una situazione di conflitto d'interessi ai sensi della regolamentazione adottata dalla Società

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

3.3.2 Verifica dei requisiti

L'Organismo di Vigilanza verifica, entro 90 giorni dalla nomina, la sussistenza, in capo ai propri componenti effettivi ed al membro supplente, dei requisiti ulteriori a quelli previsti dalla disciplina legale e regolamentare, sulla base di una dichiarazione resa dai singoli interessati, comunicando l'esito di tale verifica al Consiglio di Amministrazione.

3.3.3 Cause di decadenza

I componenti effettivi e supplenti dell'Organismo di Vigilanza, successivamente alla loro nomina, **decadono 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;
- se Sindaco della Società, incorra nella revoca o decadenza da tale carica, anche in conseguenza del venir meno dei requisiti di professionalità, onorabilità e indipendenza prescritti dalla legge o dallo Statuto;
- dopo la nomina, si accerti che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società o ente nei cui confronti siano state applicate, con provvedimento definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
- si accerti che siano stati condannati, con sentenza definitiva (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.), anche se a pena sospesa condizionalmente ai sensi dell'art. 163 c.p. per uno dei seguenti reati: reati per i quali è applicabile il D.Lgs. n. 231/2001; reati in materia di crisi d'impresa e di insolvenza[4]; delitti fiscali;
- subiscano 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. n. 58/1998 o del D. Lgs. N. 385/1993;
- sia accertata un'assenza ingiustificata a due o più riunioni consecutive dell'Organismo di Vigilanza, svoltesi a seguito di formale e regolare convocazione.

I componenti dell'Organismo di Vigilanza debbono comunicare al Presidente del Consiglio di Amministrazione, sotto la loro piena responsabilità, il sopravvenire di una delle cause di decadenza 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 causa di decadenza, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione al membro che ricopra la carica di Sindaco, convoca senza indugio il Consiglio di Amministrazione affinché proceda – nella sua prima riunione successiva all'avvenuta conoscenza – alla dichiarazione di decadenza dell'interessato dalla carica di componente dell'Organismo di Vigilanza ed alla sua sostituzione.

Nelle more dell'individuazione del membro effettivo subentrerà automaticamente il membro supplente.
In caso di decadenza del membro supplente, il Consiglio di Amministrazione provvede tempestivamente alla nomina di un nuovo supplente.

[4] Il riferimento è ai reati previsti dal R. D. n. 267/1942 e ai reati previsti dal Codice della crisi d'impresa e dell'insolvenza (D. Lgs. 14/2019).

3.3.4 Cause di sospensione

Costituiscono **cause di sospensione** dalla funzione di componente dell'Organismo di Vigilanza quelle che, ai sensi della vigente normativa di legge e regolamentare, comportano la sospensione dalla carica di Consigliere di Amministrazione ovvero di Sindaco, nonché le ulteriori di seguito riportate:

- si accerti, dopo la nomina, che i componenti dell'Organismo di Vigilanza hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a 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 commessi durante la loro carica;
- i componenti dell'Organismo di Vigilanza siano stati condannati con sentenza non definitiva e la sentenza emessa ai sensi dell'art. 444 c.p.p, anche a pena sospesa condizionalmente ai sensi dell'art. 163 c.p. per uno dei seguenti reati: reati per i quali è applicabile il D.Lgs. n. 231/2001; reati in materia di crisi d'impresa e di insolvenza[5]; per i delitti fiscali;
- il rinvio a giudizio per uno dei reati previsti al punto che precede;
- malattia o infortunio o altro giustificato impedimento che si protraggono per oltre tre mesi e impediscono al componente dell'O.d.V. di partecipare alle sedute dell'Organismo medesimo.

In tali casi il Consiglio di Amministrazione dispone la sospensione della qualifica di membro dell'Organismo di Vigilanza e la cooptazione ad interim con il membro supplente.

I componenti dell'Organismo di Vigilanza debbono comunicare al Presidente del Consiglio di Amministrazione, sotto la loro piena responsabilità, il sopravvenire di una delle cause di sospensione 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 dianzi citate, fermi gli eventuali provvedimenti da assumersi ai sensi di legge e di statuto in relazione al membro che ricopra la carica di Sindaco, convoca senza indugio il Consiglio di Amministrazione affinché provveda, nella sua prima riunione successiva, a dichiarare la sospensione del soggetto, nei cui confronti si è verificata una delle cause di cui sopra, dalla carica di componente dell'Organismo di Vigilanza. In tal caso subentra *ad interim* il membro supplente.

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

Qualora la sospensione riguardi il Presidente dell'Organismo di Vigilanza, la presidenza è assunta, per tutta la durata della medesima, dal componente più anziano di nomina o, a parità di anzianità di nomina, dal componente più anziano di età.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza del Presidente, e fino alla nomina del nuovo Presidente, le relative funzioni sono esercitate dal componente più anziano di nomina o, a parità di anzianità di nomina, dal più anziano di età, il quale rimane in carica fino alla data in cui il l'O.d.V., reintegrato con il membro supplente, non abbia provveduto all'elezione di un nuovo Presidente.

3.3.5 Temporaneo impedimento di un componente effettivo

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, ad un componente effettivo dell'Organismo di Vigilanza di svolgere le proprie funzioni ovvero di svolgerle con la necessaria indipendenza ed autonomia di giudizio, questi è tenuto a dichiarare la sussistenza del legittimo impedimento, e, qualora esso sia dovuto ad un potenziale

[5] Il riferimento è ai reati previsti dal R. D. n. 267/1942 e ai reati previsti dal Codice della crisi d'impresa e dell'insolvenza (D. Lgs. 14/2019).

conflitto di interessi, la causa da cui il medesimo deriva astenendosi dal partecipare alle sedute dell'organismo stesso o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso.
A titolo esemplificativo, costituiscono cause di temporaneo impedimento:

- la circostanza che il componente sia destinatario di un provvedimento di rinvio a giudizio in relazione ad un reato presupposto;
- la circostanza che il componente dell'Organismo apprenda dall'Autorità amministrativa di essere sottoposto alla procedura di irrogazione di una sanzione amministrativa di cui all'art. 187 quater Decreto Legislativo n. 58/1998;
- malattia o infortunio o altro giustificato impedimento che si protraggano per oltre tre mesi e impediscano di svolgere i normali compiti dell'Organismo di Vigilanza.

Nel caso di temporaneo impedimento subentra automaticamente e in via temporanea il membro supplente il quale cessa dalla carica quando viene meno la causa che ha determinato il suo subentro.

Resta salva la facoltà per il Consiglio di Amministrazione, quando l'impedimento si protragga per più di sei mesi, prorogabile di ulteriori 6 mesi per non più di due volte, di addivenire alla revoca del componente per il quale si siano verificate le predette cause di impedimento ed alla sua sostituzione con altro componente effettivo.

Qualora la sospensione o il temporaneo impedimento riguardi il Presidente, la presidenza è assunta *ad interim* dal componente effettivo più anziano di nomina o, a parità di anzianità di nomina, dal più anziano d'età.

3.4 Compiti dell'Organismo di Vigilanza

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

- sull'efficienza, efficacia ed adeguatezza del Modello nel prevenire e contrastare la commissione degli illeciti per i quali è applicabile il D.Lgs. n. 231/2001, anche di quelli che in futuro dovessero comunque comportare una responsabilità amministrativa della persona giuridica;
- sull'osservanza delle prescrizioni contenute nel Modello 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 soggetti della Società;
- sull'aggiornamento del Modello laddove si riscontrino esigenze di adeguamento, formulando proposte agli Organi della Società 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'attuazione del piano di formazione del personale, di cui al successivo cap. 6.2;
- sull'avvio e sullo svolgimento del procedimento di irrogazione di un'eventuale sanzione disciplinare, a seguito dell'accertata violazione del Modello;
- sull'adeguatezza della procedura per la segnalazione interna di condotte illecite rilevanti ai fini del D.Lgs. n.231/2001 o di violazioni del Modello e di Whistleblowing e sulla sua 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".

Per l'attività di controllo, l'Organismo di Vigilanza, segue appositi protocolli elaborati e costantemente aggiornati in base alle risultanze dell'analisi dei rischi e degli interventi di controllo e, a tale fine si avvale del supporto dell'Internal Audit al quale può richiedere lo svolgimento di specifiche verifiche.

L'analisi dei rischi è il processo continuo di identificazione, classificazione e valutazione preventiva dei rischi (esterni ed interni) e dei controlli interni, da cui discende il piano degli interventi di Audit elaborato congiuntamente con quello del Controllante.

Durante gli interventi di controllo viene analizzato nel dettaglio il livello dei controlli presenti nell'operatività e nei processi della Società. I punti di debolezza rilevati sono sistematicamente segnalati agli altri soggetti interessati, al fine di rendere più efficiente ed efficace la normativa interna e la struttura organizzativa della Società. Per verificare l'effettiva esecuzione delle azioni da intraprendere, viene poi svolta un'attività di follow-up. Di tali attività l'Internal Audit rendiconta periodicamente l'Organismo di Vigilanza.

Ai fini del Decreto, l'Organismo può richiedere all'Internal Audit di inserire nel piano annuale di audit verifiche specifiche volte, in particolare per le aree sensibili, a valutare l'adeguatezza dei controlli a prevenire comportamenti illeciti.

L'Organismo di Vigilanza può scambiare informazioni con il Collegio dei Sindaci e l'eventuale 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 al Direttore Operativo, nell'ambito delle materie di competenza del Consiglio medesimo, specifiche informazioni su temi che ritiene opportuno 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 della Società

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

Dopo l'esame da parte del Consiglio di Amministrazione, l'Organismo di Vigilanza provvede ad inoltrare l'informativa - corredata delle eventuali osservazioni formulate dal Consiglio di Amministrazione - all'Organismo di Vigilanza del Controllante.

Capitolo 4 - Flussi informativi verso l'Organismo di Vigilanza

4.1 Flussi informativi da effettuarsi al verificarsi di particolari eventi e in caso di segnalazioni Whistleblowing

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte del personale, degli Organi Statutari, dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i fornitori di servizi, ecc.) in merito ad eventi che potrebbero ingenerare responsabilità della Società ai sensi del Decreto.
Devono essere senza ritardo segnalati:

- le notizie relative alla commissione, o alla ragionevole convinzione di commissione, degli illeciti per i quali è applicabile il D.Lgs. n. 231/2001, compreso l'avvio di procedimento giudiziario a carico dei destinatari del Modello per reati previsti nel D.Lgs. n. 231/2001;
- le violazioni delle regole di comportamento o procedurali contenute nel presente Modello.

Le segnalazioni devono essere inoltrate, anche in forma anonima:

- direttamente all'Organismo di Vigilanza, tramite:
  - lettera all'indirizzo "Sommariva 14 S.r.l.", Via Monte di Pietà 34 – 10122 Torino";

  ovvero
  - e-mail agli indirizzi: odv.sommariva@intesasanpaolo.com
    odv231sommarivasrl@biemmeci.it
- per il tramite dell'Internal Audit, al quale la segnalazione potrà essere effettuata tanto direttamente quanto mediante l'eventuale responsabile gerarchico di riferimento; l'Internal Audit, esperiti i debiti approfondimenti, informa l'Organismo di Vigilanza in merito alle segnalazioni pervenute e lo rendiconta sui fatti al riguardo riscontrati.

Oltre alle segnalazioni relative alle violazioni sopra descritte, devono comunque essere immediatamente trasmesse all'Organismo, con le medesime modalità, 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 si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti ai quali è applicabile il D.Lgs. n.231/2001, qualora tali indagini coinvolgano la Società o dipendenti della Banca che operano in nome e per conto della Società od Organi Statutari della Società o comunque la responsabilità della Società stessa;
- i rapporti predisposti dai soggetti competenti nell'ambito della loro attività di controllo, dai quali possano emergere fatti, atti, eventi od omissioni con profili di grave criticità rispetto all'osservanza delle norme del Decreto;
- le iniziative sanzionatorie assunte dal Consiglio di Amministrazione.

Ciascuna soggetto 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.
L'Organismo di Vigilanza valuta le segnalazioni ricevute e eventualmente propone al Consiglio di Amministrazione i provvedimenti ritenuti congrui, 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.

Segnalazioni Whistleblowing

La LEGGE 30 novembre 2017, n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" ha l'obiettivo di incoraggiare i dipendenti a segnalare fatti o comportamenti che possano costituire una violazione dell'impianto normativo della società/ente di appartenenza, nonché ogni altra condotta irregolare di cui vengano a conoscenza, in quanto un efficace sistema interno di segnalazione (c.d. Whistleblowing) favorisce la diffusione di una cultura di legalità e rappresenta un'opportunità di miglioramento del contesto operativo sia sul piano organizzativo che etico.

Il sistema di segnalazione disciplinato dalla Legge assicura la riservatezza del segnalante, escludendo il rischio di comportamenti ritorsivi, sleali o discriminatori.

Le segnalazioni Whistleblowing riguardano qualsiasi violazione della normativa esterna e interna della Società anche non ricomprese tra gli illeciti presupposto previsti dal Legislatore nel D.Lgs.231/01, relative all'attività previdenziale, finanziaria, nonché ad ogni altra attività connessa o strumentale.

Rientrano, quindi, nell'ambito di applicazione del Whistleblowing le seguenti tipologie di segnalazioni:

- ogni violazione di politiche e/o procedure interne della Società (quali, ad esempio, lo Statuto, il Codice Etico);
- ogni condotta che dia luogo a conflitti di interesse, adottata senza aver osservato il pieno rispetto delle regole e procedure di controllo previste per tali situazioni.

Rientrano, infine, nell'ambito di applicazione del Whistleblowing gli illeciti penali, quali, ad esempio, truffa, appropriazione indebita, furto, corruzione, riciclaggio, autoriciclaggio, estorsione, frode, falso, abuso di informazioni privilegiate, trattamento illecito di dati personali, accesso abusivo a sistema informatico, false comunicazioni ad un'Autorità.

Restano escluse dalle segnalazioni ammissibili quelle aventi ad oggetto questioni interpersonali che seguiranno i canali tradizionali (ad es. responsabile gerarchico superiore).

Tali segnalazioni devono essere effettuate, dal Personale distaccato o dei soggetti esterni necessariamente in forma non anonima, con le medesime modalità sopra elencate (lettera riservata personale o e-mail) nel caso che siano venuti a conoscenza di illeciti, nonché più in generale di fatti o comportamenti che possano costituire una violazione delle norme disciplinanti l'attività della Società e ogni altra condotta irregolare.

L'Organismo di Vigilanza prenderà in considerazione le segnalazioni che presentino elementi fattuali, ne valuterà i contenuti, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali decisioni di non procedere ad una indagine interna.

La Società garantisce 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 e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

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 sia dai soggetti che svolgono attività di controllo di primo livello (coinvolte nei processi sensibili), sia dall'Internal Audit.

Flussi informativi provenienti dal Direttore Operativo

Con cadenza annuale il Direttore Operativo della Società attesta il livello di attuazione del Modello con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative, con la compilazione di un Questionario di Autodiagnosi che trasmette all'Organismo di Vigilanza. Con tale documento si evidenzia le eventuali criticità nei relativi processi, gli eventuali scostamenti rispetto al Modello o più in generale dall'impianto normativo, l'adeguatezza della medesima regolamentazione, con indicazione delle azioni e delle iniziative adottate o al piano per la soluzione.

Flussi informativi provenienti dal Legale

Il flusso di rendicontazione ordinario dal Legale verso l'Organismo di Vigilanza è incentrato su comunicazioni di eventuali variazioni intervenute nei processi e nella normativa interna, di interventi correttivi e migliorativi pianificati ed al loro stato di realizzazione, nonché eventuali estensioni dell'ambito di responsabilità amministrativa degli Enti (quest'ultima informativa deve in ogni caso essere fornita tempestivamente all'Organismo di Vigilanza).

Flussi informativi provenienti dall'Internal Audit

Il flusso di rendicontazione ordinario dell'Internal Audit verso l'Organismo stesso è incentrato sull'esito dell'attività di verifica e presidio sul sistema dei controlli interni, compresa l'adeguatezza e al funzionamento del Modello, alle va-

riazioni intervenute nei processi e nelle procedure nonché agli interventi correttivi e migliorativi pianificati e al loro stato di realizzazione.

Capitolo 5 - Il sistema sanzionatorio

Princìpi generali

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

Sulla base delle segnalazioni di illeciti pervenute ed esaminate dall'Organismo di Vigilanza, le fasi di attivazione, svolgimento e definizione del processo sanzionatorio sono affidate al Consiglio di Amministrazione della Società, che provvede poi ad informare l'Organismo di Vigilanza delle proprie determinazioni e degli esiti conseguenti.

Quanto precede verrà adottato indipendentemente dall'avvio e/o svolgimento di un'eventuale azione penale, in quanto i princìpi 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.

Caratteristiche delle sanzioni in funzione dei diversi soggetti

Personale

Si rammenta che – in attuazione delle norme statutarie del Fondo Controllante che prevedono che la Banca, in raccordo con gli altri datori di lavoro, metta gratuitamente a disposizione della Società il Direttore Operativo ed il Personale necessario al suo funzionamento – alla data di redazione ed aggiornamento del Modello, la Società non dispone di Personale dipendente, ma si avvale esclusivamente di Personale distaccato da Intesa Sanpaolo.

Pertanto, a detto Personale - nel caso venga accertata la commissione di reati eludendo fraudolentemente il Modello della Società - si applica il sistema sanzionatorio disciplinato all'interno del Modello *ex* Decreto Legislativo 231/2001 del datore di lavoro distaccante.

Soggetti esterni

I comportamenti dei soggetti esterni non conformi ai princìpi ed alle regole di condotta prescritti nel presente Modello costituiscono illecito contrattuale.

Ogni comportamento posto in essere da soggetti esterni (intendendosi per tali i professionisti, i consulenti, i fornitori, eccetera) che, in contrasto con il presente Modello, sia suscettibile di comportare il rischio di commissione di uno degli illeciti a cui 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.

Processo del sistema sanzionatorio

Alla luce di quanto premesso, il processo del sistema sanzionatorio, istituito ai sensi del Decreto, prevede:

- nei confronti dei membri degli Organi Collegiali di amministrazione e controllo della Società, la segnalazione al Consiglio di Amministrazione affinché assuma eventuali iniziative amministrative nei loro riguardi;
- nei confronti del Direttore Generale e del restante Personale distaccato la segnalazione delle infrazioni commesse al Consiglio di Amministrazione e alle competenti Funzioni del datore di lavoro distaccante; sarà cura di quest'ultimo recepire le deliberazioni della Società e applicare il sistema sanzionatorio stabilito dal proprio Codice disciplinare e dalle leggi che regolano la materia;
- nei riguardi di tutti i soggetti esterni l'applicazione delle disposizioni contrattuali e di legge che regolano la materia.

Il tipo e l'entità di ciascuna delle sanzioni stabilite saranno applicate tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione e tenuto altresì conto di even-

tuale 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.

A meri fini conoscitivi, viene di seguito riportato il sistema sanzionatorio adottato da Intesa Sanpaolo S.p.A.

Personale appartenente alle aree professionali ed ai quadri direttivi

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, 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 di Intesa Sanpaolo S.p.A. 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, 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 di Intesa Sanpaolo S.p.A. 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 e istruzioni impartite dalla direzione o dai superiori*" ai sensi di quanto previsto al **punto c)** del Codice disciplinare di Intesa Sanpaolo S.p.A. 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 di Intesa Sanpaolo S.p.A. 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 dolosità 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 di Intesa Sanpaolo S.p.A. vigente.

Personale dirigente

In caso di violazione, da parte di dirigenti, dei principi, delle regole e delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività ricomprese nelle aree sensibili di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili i provvedimenti di seguito indicati, tenuto, altresì, conto della gravità della/e violazione/i e della eventuale reiterazione. Anche in considerazione del particolare vincolo fiduciario che caratterizza il rapporto tra la Banca e il lavoratore con la qualifica di dirigente, sempre in conformità a quanto previsto dalle vigenti disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti delle imprese creditizie, finanziarie e strumentali 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 Banca, 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 l'altra 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 presente Modello.

Capitolo 6 - Formazione e comunicazione interna

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 della Società 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 organizzativi presupposto del Modello stesso, 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, etc.). Ciò affinché la conoscenza della materia e il rispetto delle regole che dalla stessa discendono costituiscano parte integrante della cultura professionale di ciascun collaboratore.

L'attività di formazione viene effettuata dalla struttura Personale di Intesa Sanpaolo. Si rammenta che il personale distaccato dalla Banca che opera presso il Fondo controllante e presso la Società risulta comunque destinatario del Modello *ex* D.Lgs. n. 231/2001 predisposto dalla Banca stessa.

6.1 Comunicazione interna

Il personale distaccato dalla Banca che inizia a lavorare per la Società riceve, il primo giorno di lavoro, copia, anche informatica o telematica, del Modello e del Codice Etico adottati da quest'ultima. La sottoscrizione di un'apposita dichiarazione attesta la consegna dei documenti, l'integrale conoscenza dei medesimi e l'impegno ad osservare le relative prescrizioni.

Nella intranet del Fondo Controllante e/o in un'apposita cartella di rete sono pubblicate e rese disponibili per la consultazione, oltre alle varie comunicazioni interne, anche il Modello di organizzazione, gestione e controllo della Società e la normativa collegata.

6.2 Formazione

Le iniziative formative sono rivolte a tutto il personale e hanno l'obiettivo, anche in funzione delle specifiche attività svolte, di illustrare i contenuti del Modello della Società e, in particolare, di sostenere adeguatamente coloro che sono coinvolti nelle attività "sensibili", oltre a creare una conoscenza diffusa e una cultura interna adeguata alle tematiche in questione, mitigando così il rischio della commissione di illeciti.

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 (formazione live, digitali);
- 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 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 degli oggetti 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 convenientemente aggiornati in relazione all'evoluzione della normativa esterna e del Modello. Se intervengono modifiche rilevanti (ad es. 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 tutto il personale cui le iniziative stesse sono dirette ed è monitorata a cura della competente struttura Personale della Banca, nonché dei soggetti competenti che devono farsi garanti, in particolare, della fruizione delle iniziative di formazione "a distanza" da parte dei loro collaboratori.

La struttura Personale di Intesa Sanpaolo ha cura di raccogliere i dati relativi alla partecipazione ai vari programmi e di conservarli in appositi archivi.

L'Organismo di Vigilanza verifica, lo stato di attuazione del piano di formazione ed 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. n. 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 2.5, le fattispecie di illeciti presupposto per le quali si applica il Decreto; con riferimento a ciascuna categoria dei medesimi sono state identificate le aree 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.

In considerazione di tutto quanto sopra e di quanto disposto dallo Statuto della Società, si rileva che nel prosieguo del presente documento sarà utilizzato indifferentemente il termine "Area" per indicare indistintamente le funzioni della Società ovvero – con riguardo alle attività svolte dalla Banca – quelle di quest'ultima.

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;
- 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 ed 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 contro il patrimonio culturale;
- 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 ed 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

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*", e il reato di "*Traffico di influenze illecite*". Sono stati previsti anche i reati di "*Corruzione tra privati*" e di "*Istigazione alla corruzione tra privati*" descritti nell'allegato "Elenco Reati" – Sezione II – Reati societari che, pur essendo ricompresi tra i reati societari ex art. 25-ter del D.Lgs. n. 231/2001, 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, nonché sono assimilabili per modalità di compimento, nonché per principi di comportamento e punti di controllo che impattano sugli stessi, alle fattispecie dei reati di "Corruzione contro la Pubblica Amministrazione" di cui all'art. 25 del D.Lgs. n. 231/2001. Pertanto, con la presente Area Sensibile si intende presidiare, oltre al rischio di commissione dei reati contro la Pubblica Amministrazione, anche il rischio di commissione dei reati di "*Corruzione tra Privati*" e "*Istigazione alla corruzione tra privati*".

Sono stati altresì aggiunti ulteriori reati posti a tutela delle pubbliche finanze, italiane e dell'Unione Europea, tra cui reati di "*Peculato*" e di "*Indebita destinazione di denaro o cose mobili*".

Ai fini del presente Modello per soggetti privati si intendono i soggetti apicali, e/o le persone loro subordinate di società controparti o in relazione con la Società.

Con riferimento alla Pubblica Amministrazione, 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 autorizzativi.

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; iv) gli Enti previdenziali e assistenziali; v) le Agenzie fiscali.

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 e i reati di "*Peculato*" e di "*Indebita destinazione di denaro o cose mobili*" presuppongono il coinvolgimento necessario di un pubblico agente, vale a dire di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" 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 certificativi[6].

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

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 in forma di S.p.A., assistente universitario, portalettere, funzionario degli uffici periferici dell'ACI, consiglieri comunali, geometra tecnico comunale, insegnanti 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, letturisti dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento della corrispondenza, dipendenti del Poligrafico dello Stato, guardie giurate che conducono furgoni portavalori.

Va considerato che la legge non richiede necessariamente, ai fini del riconoscimento in capo ad un determinato soggetto delle qualifiche pubbliche predette, la sussistenza di un rapporto di impiego con un Ente pubblico: la pubblica funzione od il pubblico servizio possono essere esercitati, in casi particolari, anche da un privato.

Deve porsi particolare attenzione al fatto che, ai sensi dell'art. 322-bis c.p., la condotta del soggetto privato – sia esso corruttore o indotto a dare o promettere utilità – è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, o 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, Organizzazioni pubbliche internazionali, o sovranazionali, Assemblee parlamentari internazionali, Corti internazionali.

Si rimanda all'Allegato "Elenco Reati", Sezione I, per un'illustrazione sintetica delle fattispecie delittuose previste dagli artt. 24 e 25 del Decreto[7] e, altresì, alla Sezione II dello stesso Allegato, ai fini dell'illustrazione sintetica del reato di "corruzione tra privati" di cui all'art. 25-ter lettera s) del Decreto.

7.2.2 Attività sensibili

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

- Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione dei contenziosi e degli accordi transattivi;
- Gestione dei rapporti con le Autorità di Vigilanza;
- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del patrimonio immobiliare e del patrimonio culturale;
- Gestione e utilizzo dei sistemi informatici e del patrimonio informativo della Società.

[7] Gli articoli 24 e 25 del D. Lgs. n. 231/2001 sono stati modificati dall'articolo 5 del D. Lgs. n. 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 FEA, di truffa e di frode informatica ai danni dell'UE.

Con riferimento all'attività sensibile concernente la "Gestione e utilizzo dei sistemi informatici e del patrimonio informativo della Società" si rimanda al protocollo 7.8.2.1.

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 interna (ove presente) che regolamenta le attività medesime.

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

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione delle attività inerenti alla richiesta di autorizzazioni o l'esecuzione di adempimenti verso alla 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, INPDAP, Direzione Provinciale del Lavoro, Medicina del Lavoro, Agenzia delle Entrate, Enti pubblici locali, ecc);
- gestione dei rapporti con Amministrazioni Statali, Regionali, Comunali o Enti locali (A.S.L., Vigili del Fuoco, Arpa, etc.) per l'esecuzione di adempimenti in materia di igiene e sicurezza e/o di autorizzazioni (ad esempio pratiche edilizie), permessi, concessioni;
- gestione dei rapporti con il Ministero dell'Economia e delle Finanze, con le Agenzie Fiscali e con gli Enti pubblici locali per l'esecuzione di adempimenti in materia di imposte;
- gestione dei rapporti con la Prefettura, la Procura della Repubblica e le Camere di Commercio competenti per la richiesta di certificati e autorizzazioni.

Ai sensi del D.Lgs. n. 231/2001, le predette attività potrebbero presentare potenzialmente occasioni per la commissione dei reati di "*Corruzione contro la Pubblica Amministrazione*", nelle sue varie tipologie, "*Induzione indebita a dare o promettere utilità*", *Traffico di influenze illecite*"[8] e di "*Truffa ai danni dello Stato o di altro Ente Pubblico*".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del processo

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

- predisposizione della documentazione;
- invio della documentazione richiesta e archiviazione della pratica;
- gestione dei rapporti con gli Enti pubblici;
- assistenza in occasione di sopralluoghi ed accertamenti da parte degli Enti;

[8] 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 riguardi: 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 gli Enti pubblici per il ritiro dell'autorizzazione e l'esecuzione degli adempimenti.

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - tutti i soggetti che intervengono nella gestione delle attività inerenti alla richiesta di autorizzazioni o all'esecuzione di adempimenti verso la Pubblica Amministrazione sono individuati e, ove richiesto, autorizzati da parte del Direttore Operativo della Società; 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 Funzionari pubblici in caso di accertamenti/sopralluoghi, effettuati anche allo scopo di verificare l'ottemperanza alle disposizioni di legge che regolamentano l'operatività dell'area di propria competenza, è attribuita al Direttore Operativo della Società e/o ai soggetti da quest'ultimo appositamente individuati.

- Segregazione dei compiti tra i soggetti operativamente coinvolti nel processo di gestione delle attività inerenti alla richiesta di autorizzazioni o all'esecuzione di adempimenti verso la Pubblica Amministrazione e il Direttore Operativo della Società, al fine di garantire, per tutte le fasi del processo un meccanismo di maker e checker.

- Attività di controllo: le attività devono essere svolte in modo tale da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell'istanza di autorizzazione o forniti in esecuzione degli adempimenti, prevedendo, ove opportuno, specifici controlli in contraddittorio. In particolare, laddove l'autorizzazione/adempimento preveda l'elaborazione di dati ai fini della predisposizione dei documenti richiesti dall'Ente pubblico, è effettuato un controllo sulla correttezza delle elaborazioni da parte di soggetti diversi da quelli deputati alla esecuzione delle attività, ad eccezione delle eventuali successive richieste di integrazione avanzate dall'Ente pubblico, che sono eseguite direttamente ed esclusivamente dal Service esterno.

- 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 dai soggetti competenti;
  - il Direttore Operativo della Società, 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, di inviarne una copia all'Internal Audit 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, i soggetti di volta in volta interessati sono responsabili 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

I soggetti, a qualsiasi titolo coinvolti nella gestione dei rapporti con la Pubblica Amministrazione in occasione di richiesta di autorizzazioni o esecuzione di adempimenti, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della 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 segnalarli al Direttore Operativo della Società, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi (professionisti, ditte, ecc.) nell'espletamento delle attività inerenti alla richiesta di autorizzazioni ovvero l'esecuzione di adempimenti verso la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dal Direttore Operativo della Società; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

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

- 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 ad omettere informazioni dovute o a compiere un atto contrario ai doveri d'ufficio costituente reato dal quale possa derivare un vantaggio indebito 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 sè o per altri – a soggetti della Pubblica Amministrazione, con la finalità di promuovere o favorire interessi della Società;
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili e obiettivi quali professionalità e competenza, competitività, prezzo, integrità 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; ciò al fine di prevenire il rischio di commissione dei reati di corruzione, nelle sue 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 alla conseguente possibilità di agevolare/condizionare la gestione del rapporto con la Società.

I soggetti interessati 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.

7.2.2.2. Gestione dei contenziosi e degli accordi transattivi

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione dei contenziosi giudiziali e stragiudiziali (amministrativo, civile, penale e fiscale) e degli accordi transattivi con Enti Pubblici o con soggetti privati.

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "*Corruzione contro la Pubblica Amministrazione*", nelle sue varie tipologie, "*Corruzione in atti giudiziari*", "*Induzione indebita a dare o promettere utilità*", "*Traffico di influenze illecite*"[9] e "*Truffa ai danni dello Stato o di altro Ente Pubblico*", nonché del reato di "*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*"[10].
Sussiste altresì il rischio della commissione dei reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del Processo

Il processo di gestione del contenzioso si articola nelle seguenti fasi, effettuate sotto la responsabilità dei soggetti competenti per materia, in coordinamento con i soggetti interessati dalla controversia e con gli eventuali professionisti esterni incaricati:

- apertura del contenzioso giudiziale o stragiudiziale:
  - raccolta delle informazioni e della documentazione relative alla vertenza;
  - analisi, valutazione e produzione degli elementi probatori;

[9] 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 riguardi: 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.

[10] Tale reato, 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.

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

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

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

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti:
  - il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni, nonché le facoltà di autonomia in merito alla gestione del contenzioso, ivi incluso quello nei confronti della Pubblica Amministrazione;
  - la documentazione da fornire all'Autorità Amministrativa e Giudiziaria è predisposta dal soggetto competente, con il supporto, ove necessario, di eventuali professionisti esterni, ed è autorizzata, prima dell'invio, dal Presidente;
  - il conferimento degli incarichi a legali esterni diversi da quelli individuati nell'ambito dell'albo predisposto e approvato dal Consiglio di Amministrazione della Società è autorizzato dal Presidente.

- 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, con relativa informativa al Consiglio di Amministrazione in merito agli sviluppi delle stesse;

- 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, i soggetti interessati sono altresì responsabili 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

I soggetti, a qualsiasi titolo coinvolti nella gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico. In particolare:

- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla 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. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dal Direttore Operativo della Società; in ogni caso non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarli al Direttore Operativo della Società, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso.

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

- in sede di contatti formali o 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 – i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero ad omettere informazioni dovute o a compiere un atto contrario ai doveri d'ufficio costituente reato dal quale possa derivare un vantaggio indebito al fine di influenzare impropriamente la gestione del rapporto con la Società;
- promettere o versare/offrire – anche a mezzo di intermediari – somme di denaro non dovute, doni o gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), o accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri – a favore di soggetti della Pubblica Amministrazione, di esponenti apicali o persone a loro subordinate appartenenti a società controparti o in relazione con la Società, al fine di favorire indebitamente gli interessi della Società, oppure minacciarli di un danno ingiusto per le medesime motivazioni;
- affidare incarichi a professionisti esterni eludendo criteri documentabili ed obiettivi, quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del professionista devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico; ciò al fine di prevenire il rischio di commissione del reato di corruzione, nelle sue varie tipologie, di induzione indebita a dare o promettere utilità, di traffico di influenze illecite e di 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/condizionare il rapporto con la Società.

I soggetti interessati 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.

7.2.2.3. Gestione dei rapporti con le Autorità di Vigilanza

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione dei rapporti con le Autorità di Vigilanza e riguarda qualsiasi tipologia di attività posta in essere in occasione di segnalazioni, adempimenti, comunicazioni, richieste e visite ispettive.

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe presentare potenzialmente occasioni per la commissione dei reati di "*Corruzione contro la Pubblica Amministrazione*", nelle sue varie tipologie, "*Induzione indebita a dare o promettere utilità*", "*Traffico di influenze illecite*"[11], "*Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza*" (art. 2638 del codice civile) e "*Frode informatica*".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del Gruppo Intesa Sanpaolo, sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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 (a titolo esemplificativo, Autorità Garante per la Privacy).

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

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del Processo

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

- elaborazione/trasmissione delle segnalazioni occasionali o periodiche alle Autorità di Vigilanza;
- richieste/istanze di abilitazioni e/o autorizzazioni;
- 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.

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica del processo. In particolare:
  - ad eccezione delle visite ispettive i rapporti con le Autorità di Vigilanza sono intrattenuti dal Direttore Operativo della Società e/o da soggetti dallo stesso appositamente incaricati;
  - gli atti che impegnano contrattualmente la Società devono essere sottoscritti soltanto da soggetti incaricati.

[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 riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, o 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.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con le Autorità di Vigilanza. In particolare:
  - tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell'operatività interna indirizzata alle Autorità di Vigilanza è preventivamente condivisa con l'Internal Audit e/o il referente del Legale;
  - è compito del Direttore Operativo della Società, dopo aver accertato l'oggetto dell'ispezione, individuare le risorse deputate a gestire i rapporti con i Funzionari pubblici durante la loro permanenza presso la Società. L'Internal Audit deve essere tempestivamente informato della visita ispettiva in atto e di eventuali prescrizioni o eccezioni rilevate dall'Autorità, e darne a sua volta comunicazione all'Organismo di Vigilanza.
- Attività di controllo:
  - controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle Autorità di Vigilanza da parte soggetti interessati per le attività di competenza;
  - controlli di carattere giuridico sulla conformità alla normativa di riferimento della segnalazione/comunicazione richiesta.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - è fatto obbligo a tutti i soggetti, a vario titolo coinvolti 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 all'Internal Audit e/o all'Organismo di Vigilanza;
  - ogni comunicazione nei confronti delle Autorità avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Società è documentata in via informatica ed archiviata da parte dei soggetti competenti;
  - 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 rappresentanti delle Autorità di Vigilanza i soggetti interessati provvedono a trasmettere all'Internal Audit 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 all'Internal Audit. La suddetta documentazione è archiviata dai medesimi soggetti.

Principi di comportamento

I soggetti, a qualsiasi titolo coinvolti nel processo di gestione dei rapporti con le Autorità di Vigilanza, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico. In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della 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 dell'Autorità di Vigilanza di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarli al Direttore Operativo della Società, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso;
- devono essere puntualmente trasmesse le segnalazioni periodiche alle Autorità di Vigilanza e 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.

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

- 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 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 ad omettere informazioni dovute o a compiere un atto contrario ai doveri d'ufficio costituente reato dal quale possa derivare un vantaggio indebito 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, con la finalità di promuovere o favorire interessi della Società.

I soggetti interessati 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.

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

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione delle procedure acquisitive dei beni e dei servizi.
Tra i beni vanno considerate anche le opere dell'ingegno di carattere creativo[12], mentre tra le prestazioni vanno ricomprese anche quelle a contenuto intellettuale di qualsiasi natura (es.: legale, fiscale, tecnica, amministrativa, organizzativa, ecc.), ivi incluso il conferimento di incarichi professionali ovvero di consulenze.

Ai sensi del D.Lgs. n. 231/2001, il relativo processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "*Corruzione contro la Pubblica Amministrazione*", nelle sue varie tipologie, "*Induzione indebita a dare o promettere utilità*" e "*Traffico di influenze illecite*"[13].
Sussiste altresì il rischio della commissione dei reati di "*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.

Sussistono altresì profili di rischio potenzialmente connessi alla commissione dei reati con "*finalità di terrorismo o di eversione dell'ordine democratico*", di "*Criminalità organizzata*", "*Transnazionali*", reati "*contro la personalità individuale*", di "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*"[14], di "*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*", "*Reati contro l'industria e il commercio*", reati "*in materia di violazione del diritto d'autore*" e "*Reati di contrabbando*"[15], che si intendono presidiare anche attraverso il presente protocollo.

Con riferimento alle modalità procedurali in materia di gestione della spesa e di assegnazione dei lavori, si rimanda all'integrazione dello specifico mandato conferito alla società terza, avente ad oggetto l'amministrazione del patrimonio immobiliare della Società.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del Processo

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

- gestione del ciclo passivo;
- gestione dei fornitori.

[12] Ai sensi dell'art. 2575 del codice civile, le opere dell'ingegno di carattere creativo tutelate dal diritto d'autore sono quelle che appartengonoalle scienze, 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).

[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 riguardi: i) quei soggetti espletanti funzioni o attività corrispondenti nell'ambito delle Istituzioni o degli organi dell'UE, o 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] Si veda a riguardo il paragrafo 7.4.

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

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti:
  - il conferimento dell'incarico ed il perfezionamento del contratto 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. L'approvazione della richiesta d'acquisto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere, nonché alla Banca per le spese oggetto di refusione da parte della stessa. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
  - la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati in base a criteri individuati nell'ambito della normativa, fatte salve esigenze/forniture occasionali. Tali soggetti devono garantire e su richiesta poter documentare, anche con riferimento ai subappaltatori da loro incaricati:
    - in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi, il rispetto della disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti;
    - in relazione ai lavoratori impiegati, il rispetto della disciplina in tema di immigrazione e la regolarità retributiva, contributiva, previdenziale, assicurativa e fiscale;
  - l'autorizzazione al pagamento della fattura spetta al Direttore Operativo della Società, per il quale è prevista l'assegnazione di un budget e delle relative facoltà di spesa o ai soggetti all'uopo incaricati; può essere negata a seguito di formale contestazione delle inadempienze/carenze della fornitura adeguatamente documentata e dettagliata a cura dei competenti soggetti;
  - il pagamento delle fatture è effettuato dai soggetti di volta in volta competenti.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle procedure acquisitive. In particolare, le attività di cui alle diverse fasi del processo devono essere svolte da soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.
- Attività di controllo: ciascun soggetto interessato in ogni singola fase del processo verifica, per quanto di propria competenza:
  - i limiti di spesa e la pertinenza della stessa;
  - la regolarità, completezza, correttezza e tempestività delle scritture contabili;
  - il rispetto dei criteri individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti, ivi comprese le garanzie circa l'autenticità e la legittima provenienza dei beni forniti;
  - il rispetto delle norme di legge che vietano o subordinano a determinate condizioni il conferimento di incarichi di qualunque tipologia a dipendenti pubblici o ex dipendenti pubblici.

Per quanto concerne infine il conferimento di incarichi professionali e consulenze il cui svolgimento comporta un rapporto diretto con la Pubblica Amministrazione (quali ad esempio spese legali per contenzioso, ecc.) i soggetti deputati delle Aree 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 succitato elenco al fine di individuare eventuali situazioni anomale.

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

- utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
- documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista, in termini di motivazione della scelta nonché pertinenza e congruità della spesa. Con riferimento all'amministrazione del patrimonio immobiliare della Società, il relativo mandato conferito alla Società terza individua in quali casi l'individuazione del fornitore di beni e/o servizi o professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, i soggetti di volta in volta interessati sono responsabili dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.

Principi di comportamento

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

- la documentazione contrattuale che regola il conferimento di incarichi di fornitura/incarichi professionali deve contenere un'apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dal Direttore Operativo della Società; 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;
- 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 segnalarli al Direttore Operativo della Società, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso.

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

- assegnare incarichi di fornitura ed incarichi professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;
- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori 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;
- promettere o 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) 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, oppure minacciarli di un danno ingiusto per le medesime motivazioni.

I soggetti interessati 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 di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni.

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

- per omaggi si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine della 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 iniziative di beneficenza si intendono le elargizioni in denaro che la Società destina esclusivamente ad Enti senza fini di lucro;
- 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*"[16], nonché i reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Sussistono altresì profili di rischio potenzialmente connessi alla commissione dei reati con "*finalità di terrorismo o di eversione dell'ordine democratico*", di "*Criminalità organizzata*", "*Transnazionali*", di "*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*", che si intendono presidiare anche attraverso il presente protocollo.

Una gestione non trasparente dei processi relativi a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali, e/o a persone loro subordinate, di società o enti controparti o in relazione con la Società, 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 risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

[16] Si ricorda che, ai sensi dell'art. 322 *bis* c.p., la condotta del corruttore, istigatore e del soggetto che cede all'induzione è penalmente sanzionata non solo allorché coinvolga i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio nell'ambito della Pubblica Amministrazione italiana, ma è pure considerata illecita ed allo stesso modo è punita anche quando riguardi: 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, 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, ecc.) 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".

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

- ricezione della richiesta, inviata dagli Enti, di elargizioni e di beneficenze o sponsorizzazioni per progetti, iniziative, manifestazioni;
- individuazione di società/organizzazioni cui destinare le elargizioni;
- effettuazione delle attività di due diligence[17] 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 di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti:
  - per quanto attiene ai beni destinati ad omaggi ed alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
  - tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
  - nel caso in cui le attività siano realizzate da soggetti terzi – che operano in nome o per conto della Società – questi ultimi vengono individuati con lettera di incarico/nomina ovvero nell'ambito dei contratti stipulati dalla Società, nei limiti della normativa applicabile e secondo le modalità della stessa previste;
  - 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, nonché della natura dell'omaggio stesso[18], e comunque

[17] 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.

[18] Si fa riferimento, a titolo esemplificativo, a situazioni in cui gli omaggi siano componenti di offerte a prevalente contenuto professionale, quali inviti a conferenze e seminari.

nei limiti della ragionevolezza, previa autorizzazione del soggetto responsabile. I limiti di importo previsti, su base annua per gli omaggi e altre utilità, non si applicano alle spese di rappresentanza relative eventi e forme di accoglienza ed ospitalità (inclusi pranzi, cene) che vedano la partecipazione di esponenti aziendali e personale della Società, purché strettamente inerenti al rapporto di affari istituzionale e ragionevoli rispetto alle prassi di cortesia commerciale e/o istituzionale comunemente accettate;

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

- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi. In particolare:
  - le attività di cui alle diverse fasi dei processi devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.

- Attività di controllo:
  - la normativa interna definisce le modalità con le quali le erogazioni relative a beneficenze (ivi compresi i casi di adesione, effettuata con intento di liberalità, a fondazioni, associazioni e altri enti non aventi scopo di lucro, che comporti l'erogazione di fondi o impegni futuri in tal senso) e sponsorizzazioni devono essere precedute da un'attività di due diligence da parte dei soggetti interessati. In particolare, è prevista l'analisi e la verifica del tipo di organizzazione e della finalità per la quale è costituita:
    - verifica ed approvazione di tutte le erogazioni da parte del Direttore Operativo della Società;
    - verifica che le erogazioni complessive siano stabilite annualmente e trovino capienza in apposito budget deliberato dagli Organi competenti;
  - per le sponsorizzazioni è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa.

  Inoltre, i soggetti competenti dovranno:
  - disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi distribuiti nonché le relative date/occasioni di elargizioni. Tale obbligo non si applica per gli omaggi cosiddetti "marchiati", riportanti cioè il logotipo della Società (quali biro, oggetti per scrivania, ecc.);
  - verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione, da parte di tutti i soggetti interessati, di una reportistica sulle erogazioni effettuate/contratti stipulati;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, i soggetti di volta in volta interessati sono responsabili dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni;
  - qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo in oggetto, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto.

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, i soggetti a qualsiasi titolo coinvolti nella gestione di omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni

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

- la Società può effettuare beneficenze o sponsorizzazioni per sostenere iniziative di enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici della Società e nel caso di beneficenze, tali enti non devono avere finalità di lucro;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le "sponsorizzazioni" non possono essere oggetto contemporaneo di erogazione per beneficenza;
- i pagamenti devono essere riconosciuti esclusivamente su un conto corrente intestato all'ente beneficiario; non è consentito effettuare pagamenti in contanti, né pagamenti in un Paese diverso da quello dell'ente beneficiario o a un soggetto diverso dallo stesso[19].

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

- effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di enti coinvolti 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 Direttore Operativo della Società;
- effettuare elargizioni/omaggi a favore di enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate contravvenendo a quanto previsto nel presente protocollo;
- promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi della 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 segnalarli al Direttore Operativo della Società, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso;
- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con la Società, al fine di favorire indebitamente gli interessi della Società;
- 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.;
- dare in omaggio somme di denaro o strumenti assimilabili (quali carte regalo e buoni acquisto).

[19] In materia di sponsorizzazioni, i pagamenti possono essere eseguiti a favore dell'eventuale Beneficiario Amministrativo indicato contrattualmente dallo Sponsee, ferma restando la due diligence anche su quest'ultimo.

I soggetti interessati 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 del patrimonio immobiliare e del patrimonio culturale

Premessa

La gestione del patrimonio immobiliare e del patrimonio culturale - intendendosi per tale l'insieme di beni mobili e immobili ai sensi del D. Lgs. 42/2004[20] - riguarda qualunque tipologia di attività svolta dalla Società finalizzata alla valorizzazione ed ottimizzazione del patrimonio immobiliare, di proprietà ed in locazione, nonché alla valorizzazione, valutazione degli interventi e gestione del patrimonio culturale della Società.

Ai sensi del D.Lgs. n. 231/2001, il processo in oggetto potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "*Corruzione contro la Pubblica Amministrazione*", nelle sue varie tipologie, "*Induzione indebita a dare o promettere utilità*", "*Traffico di influenze illecite*"[21], "*Truffa ai danni dello Stato o di altro Ente pubblico*", nonchè dei reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Una gestione non trasparente del processo relativo alla gestione del patrimonio immobiliare e del patrimonio culturale della Società potrebbe, infatti, consentire la commissione di tali reati, attraverso il riconoscimento / concessione di vantaggi ad esponenti della Pubblica Amministrazione ovvero a esponenti apicali e/o a persone a loro subordinate appartenenti a società o enti privati al fine di favorire interessi della Società.

Sussiste altresì il rischio di commissione dei reati contro il patrimonio culturale e paesaggistico che prevedono la responsabilità amministrativa dell'ente in relazione alla commissione dei reati di "*Furto di beni culturali*", "*Appropriazione indebita di beni culturali*", "*Importazione illecita di beni culturali*", "*Uscita o esportazione illecite di beni culturali*", "*Violazioni in materia di alineazione di beni culturali*", "*Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali e paesaggistici*", "*Contraffazione di opere d'arte*", "*Ricettazione di beni culturali*", "*Falsificazione in scrittura privata relativa a beni culturali*", "*Riciclaggio di beni culturali*" e "*Devastazione e saccheggio di beni culturali e paesaggistici*", in riferimento ai quali si rimanda all'"Area sensibile concernente i reati contro il patrimonio culturale".

Sussistono, inoltre, profili di rischio potenzialmente connessi alla commissione dei reati con "*finalità di terrorismo o di eversione dell'ordine democratico*", di "*Criminalità organizzata*", di "*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*", che si intendono presidiare anche attraverso il presente protocollo.

I soggetti incaricati della gestione della documentazione ai fini dell'ottenimento di autorizzazioni/certificazioni/nullaosta rilasciati dalla Pubblica Amministrazione, sono tenuti 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".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

---

[20] Ai sensi dell'art. 2 del Codice dei beni culturali e del paesaggio il patrimonio culturale è costituito dai beni culturali (le cose immobili e mobili che presentano interesse artistico, storico, archeologico, etnoantropologico, archivistico e bibliografico e le altre cose individuate dalla legge o in base alla legge quali testimonianze aventi valore di civiltà (ex artt. 10 e 11) e paesaggistici (immobili e le aree indicati all'articolo 134, costituenti espressione dei valori storici culturali, naturali, morfologici ed estetici del territorio, e gli altri beni individuati dalla legge o in base alla legge).

[21] 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 riguardi: 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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del processo

L'attività di gestione del patrimonio immobiliare e del patrimonio culturale della Società si articola nei seguenti processi:

- pianificazione degli atti dispositivi;
- gestione amministrativa e contabile degli immobili;
- gestione dei contratti locazione;
- gestione delle spese di proprietà e degli oneri fiscali.

In particolare, la gestione del patrimonio immobiliare prevede:

- l'individuazione e selezione opportunità di investimento/disinvestimento;
- l'acquisizione e vendita degli immobili;
- l'ottimizzazione del patrimonio immobiliare corrente;
- la pianificazione immobiliare di lungo periodo;
- la progettazione, manutenzione ed esecuzione lavori.

Gestione del patrimonio culturale (Beni mobili e beni immobili e apparati decorativi soggetti a tutela[22]):

- acquisizione dei beni rivenienti da operazioni societarie (fusioni, incorporazioni), donazioni, acquisto sul mercato;
- gestione contratti di prestito/locazione;
- cessione anche a titolo non oneroso;
- gestione delle attività inerenti alla ricognizione, al censimento, alla conservazione, alla manutenzione e dei connessi adempimenti nei confronti della Pubblica Amministrazione;
- gestione degli incidenti (smarrimento, sottrazione, deterioramento, danneggiamento, distruzione, uso improprio).

Le modalità operative di base per la gestione dei processi sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi definiti:
  - tutti i soggetti che intervengono nella gestione del patrimonio immobiliare e del patrimonio culturale con la Pubblica Amministrazione sono individuati e, ove richiesto, autorizzati dal Direttore Operativo della Società;
  - la definizione degli accordi è esclusivamente affidata al Direttore Operativo della Società o a soggetti dal medesimo appositamente incaricati;
  - tutte le deliberazioni relative alle compravendite, alle donazioni, alle cessioni a titolo non oneroso, alle locazioni e alle concessioni in comodato, ai prestiti e cessione del diritto di superficie anche a titolo non oneroso spettano esclusivamente a soggetti muniti di idonei poteri in base al vigente sistema dei poteri e delle deleghe che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno, ivi inclusi quelli nei confronti della Pubblica Amministrazione.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo. In particolare:
  - le attività di cui alle diverse fasi del processo sono svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker;

[22] Per quanto attiene ai beni immobili e apparati decorativi appartenenti al patrimonio culturale si richiamano altresì i processi sopraindicati relativi alla gestione del patrimonio immobiliare.

- separazione delle attività relative alla:
  - definizione delle esigenze di copertura del territorio e individuazione degli immobili da locare/dismettere;
  - definizione del prezzo di mercato e stipulazione dei contratti;
  - gestione amministrativa;
  - gestione finanziaria.

- Attività di controllo:
  - verifica della congruità del canone di locazione attiva per tutte le nuove locazioni e le rinegoziazioni di locazioni con riferimento alle condizioni espresse dal mercato, attraverso l'acquisizione di perizie redatte da esperti indipendenti ogni qualvolta la controparte sia una Pubblica Amministrazione o un esponente della medesima ovvero un esponente apicale o una persona allo stesso subordinata appartenente a una società privata;
  - effettuazione delle attività di due diligence sulla controparte;
  - verifica della congruità del prezzo di compravendita dell'immobile rispetto al valore di mercato, attraverso l'acquisizione di perizie redatte da esperti indipendenti ogni qualvolta la controparte sia una Pubblica Amministrazione o un esponente della medesima ovvero un esponente apicale o una persona allo stesso subordinata appartenente a una società privata;
  - verifica puntuale di tutti i dati contenuti nei contratti di compravendita e, in particolare, verifica di coerenza tra compromesso / preliminare e contratto definitivo;
  - redazione e aggiornamento dell'anagrafe delle locazioni in essere, con indicazione di dettaglio delle nuove locazioni e di quelle oggetto di rinnovo nel periodo di riferimento
  - redazione e aggiornamento dell'anagrafe dei beni mobili appartenenti al patrimonio culturale e della documentazione classificata negli archivi storici;
  - verifica per tutti i beni del patrimonio culturale oggetto di acquisizione dell'esistenza di:
    - una perizia redatta da un esperto indipendente attestante la legittima provenienza e l'autenticità dei beni mobili culturali o della dichiarazione della Sovrintendenza archivistica e bibliografica attestante l'interesse storico particolarmente importante dei beni archivistici;
    - una perizia per i beni immobili tutelati con l'indicazione dei vincoli diretti;
  - verifica al momento della cessione, anche a titolo non oneroso, ovvero della donazione dei beni del patrimonio culturale della Società, dell'esistenza della perizia o della dichiarazione della Sovrintendenza archivistica e bibliografica di cui al punto precedente, dell'ottenimento delle autorizzazioni previste, del corretto espletamento delle denunce alle Autorità competenti e del rispetto dei termini di prelazione a favore del Ministero o, nel caso della Regione o di altro ente pubblico territoriale interessato;
  - verifica, in caso di trasferimento all'estero di beni mobili appartenenti al patrimonio culturale della Società, dell'esistenza attestato di libera circolazione o licenza di esportazione;
  - verifica dell'ottenimento delle autorizzazioni previste dalle Autorità competenti prima di procedere ad interventi sui beni soggetti a vincoli culturali o paesaggistici.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ciascuna fase rilevante inerente agli atti dispositivi (compravendite, locazioni, prestiti, cessioni anche a titolo non oneroso, donazioni e comodati) deve risultare da apposita documentazione scritta;
  - ogni atto dispositivo (compravendite, locazioni, prestiti, cessioni anche a titolo non oneroso, donazioni e comodati) 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 delle scelte effettuate, i soggetti di volta in volta interessati sono responsabili dell'archiviazione e della conservazione della documentazione di

competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di gestione del patrimonio immobiliare e del patrimonio culturale.

Principi di comportamento

I soggetti, a qualsiasi titolo coinvolti nella gestione del patrimonio immobiliare e del patrimonio culturale della Società, sono tenuti ad osservare le modalità esposte nel presente documento, le previsioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico.

In particolare:

- tutti i soggetti che, in fase di identificazione di nuove opportunità di investimento / disinvestimento, intrattengono rapporti con la Pubblica Amministrazione per conto della Società, devono essere espressamente autorizzati;
- 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 segnalarli al Direttore Operativo della Società, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso;
- qualora sia previsto il coinvolgimento di soggetti terzi nel processo di gestione del patrimonio immobiliare e culturale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dal Direttore Operativo della Società; 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;
- la sottrazione, lo smarrimento, il deterioramento, il danneggiamento, la distruzione e l'uso improprio - oppure tale da recare pregiudizio alla loro conservazione - dei beni del patrimonio culturale della Società devono essere immediatamente comunicati.

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- creare, in tutto o in parte, una scrittura privata falsa o, alterare, distruggere, sopprimere od occultare una scrittura privata vera, in relazione a beni culturali al fine di farne apparire lecita la provenienza;
- promettere o concedere beni immobili e beni culturali – anche a mezzo di intermediari – a Enti della Pubblica Amministrazione, istituzioni pubbliche o a soggetti da questi ultimi indicati a condizioni diverse da quelle di mercato;
- promettere o concedere beni immobili e beni culturali a esponenti apicali, e/o persone a loro subordinate, di società controparti o in relazione con la Società ovvero a soggetti da questi indicati, al fine di favorire indebitamente il perseguimento di interessi della Società;
- procedere all'autorizzazione al pagamento di fatture passive in assenza di un'attenta e puntuale verifica dell'importo da liquidare;
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi, quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico; ciò al fine di prevenire il rischio di commissione di reati di "*Corruzione*", nelle sue varie tipologie, di "*Induzione indebita a dare o promettere utilità*", "*Traffico di influenze illecite*" e di "*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 sottoposte appartenenti a società private e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Società;

- trasferire all'estero beni mobili appartenenti al patrimonio culturale della Società senza attestato di libera circolazione o licenza di esportazione;
- porre in circolazione, come autentici, esemplari contraffatti, alterati o riprodotti di beni mobili appartenenti al patrimonio culturale della Società.

I soggetti interessati 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 Area sensibile concernente i reati societari

7.3.1 Fattispecie di reato

Premessa

L'art. 25-*ter* del D.Lgs. n. 231/2001 contempla quasi tutti i reati societari previsti dal Titolo XI del codice civile, che sono qualificabili come reati generali, in quanto non specificamente riferibili all'esercizio della specifica attività della Società[23]. La L. n. 190/2012, cosiddetta "legge anticorruzione", entrata in vigore il 28.11.2012, ha modificato l'art. 25-*ter*, aggiungendo il riferimento al nuovo reato di "Corruzione tra privati", previsto dall'art. 2635, comma 3, c.c.
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 rimanda all'Allegato "Elenco Reati", Sezione II, per un'illustrazione sintetica delle fattispecie delittuose previste dall'art. 25-ter del Decreto.

7.3.2 Attività 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 Collegio dei Sindaci e con la Società di Revisione;
- Gestione dell'informativa periodica;
- Gestione dei rapporti con le Autorità di Vigilanza.

Si riportano di seguito, per le prime due sopraelencate attività sensibili, i protocolli che dettano i principi di controllo ed i principi di comportamento applicabili a dette attività e che si completano con la normativa interna che regolamenta le attività medesime (ove presente).

Per quanto concerne il reato di corruzione tra privati, trattandosi di fattispecie a potenziale impatto trasversale anche su altre attività della Società, si rimanda altresì alle attività sensibili già oggetto dei seguenti protocolli predisposti nell'ambito della "Area sensibile concernente i reati contro la Pubblica Amministrazione" (paragrafo 7.2):

- Gestione dei contenziosi e degli accordi transattivi;
- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del patrimonio immobiliare e del patrimonio culturale.

in quanto contenenti principi che esplicano la loro efficacia preventiva anche in relazione al reato suddetto.

Infine, relativamente all'attività indicata al terzo punto si rimanda al protocollo per la "*Gestione dei rapporti con le Autorità di Vigilanza*", avente la specifica finalità di prevenire, oltre al reato di corruzione, anche il reato societario di cui all'art. 2638 c.c.

[23] L'art. 25 *ter* è stato modificato da:
- L. 190/12, 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. 69/15, 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.

7.3.2.1. Gestione dei rapporti con il Collegio dei Sindaci e con la Società di Revisione

Premessa

Il presente protocollo si applica ai membri del Consiglio di Amministrazione e a tutti gli Organi e i soggetti coinvolti nella gestione dei rapporti con il Collegio dei Sindaci in essere e con la Società di Revisione in occasione di verifiche e di controlli svolti, in ottemperanza alle prescrizioni di legge.

Ai sensi del D.Lgs. n. 231/2001, il processo in oggetto potrebbe presentare potenzialmente occasioni per la commissione del reato di "*Impedito controllo*", ai sensi dell'art. 2625 del codice civile nonché del reato di cui all'art. 29 del D.Lgs. n. 39/2010 (concernente la fattispecie di impedimento od ostacolo alle attività di revisione legale) che - nonostante quanto affermato nel precedente paragrafo 7.3.1 - viene comunque tenuto in considerazione ai fini del presente protocollo.

Limitatamente alla gestione dei rapporti con la Società di Revisione, sussiste altresì il rischio della commissione del reato di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Si rileva che la Società ha deciso di affidare la revisione contabile del proprio Bilancio, su base legale, ad una società di revisione.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del Processo

Nell'ambito dell'attività di verifica propria del Collegio dei Sindaci 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 relativi alla Società e messa a disposizione della documentazione, sulla base delle richieste ricevute.

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante 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 Collegio dei Sindaci e la Società di Revisione sono intrattenuti dal Direttore Operativo della Società e/o dai soggetti dal medesimo appositamente incaricati.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con il Collegio dei Sindaci 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 Collegio dei Sindaci alle riunioni del Consiglio di Amministrazione, a garanzia della effettiva conoscenza da parte dell'Organo di Controllo in merito alle scelte operate dalla Società.

- Tempestiva e completa evasione, da parte dei soggetti di volta in volta interessati, delle richieste di documentazione specifica avanzate dal Collegio dei Sindaci nell'espletamento della propria attività di vigilanza e controllo.
- Tempestiva e completa evasione, a cura dei soggetti 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: ciascun soggetto competente 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 dei soggetti di volta in volta interessati, 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 Collegio dei Sindaci;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, i soggetti di volta in volta interessati sono responsabili dell'archiviazione e della conservazione della documentazione prodotta tramite estrazioni informatiche, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla gestione dei rapporti con il Collegio dei Sindaci e la Società di Revisione.

Principi di comportamento

I soggetti e gli Organi della Società, a qualsiasi titolo coinvolti nella gestione dei rapporti con il Collegio dei Sindaci 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.

In particolare:

- devono essere puntualmente trasmesse le comunicazioni periodiche inerenti al Bilancio al Collegio dei Sindaci e alla Società di Revisione e tempestivamente riscontrate le richieste/istanze pervenute dagli stessi;
- i membri del Consiglio di Amministrazione ed i soggetti che, a qualunque titolo, siano coinvolti in una richiesta di produzione di documenti o di informazioni da parte del Collegio dei Sindaci o da qualunque dei suoi membri nonché 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;
- ciascun soggetto di volta in volta interessato è responsabile dell'archiviazione e della conservazione di tutta la documentazione formalmente prodotta e/o consegnata ai membri del Collegio dei Sindaci 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. n. 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 Collegio dei Sindaci e la Società di Revsione in errore di valutazione tecnico-economica della documentazione presentata;
- promettere o dare somme di denaro non dovute o altre utilità a membri del Collegio dei Sindaci o della Società di Revisione con la finalità di promuovere o favorire interessi della Società.

I soggetti interessati 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 tutti soggetti coinvolti nella predisposizione dei documenti che contengono comunicazioni relative alla situazione economica, patrimoniale e finanziaria della Società.

Ai sensi del D.Lgs. n. 231/2001, il processo di predisposizione dei documenti in oggetto potrebbe presentare potenzialmente occasioni per la commissione del reato di "*False comunicazioni sociali*", così come disciplinato agli artt. 2621 e 2622 del Codice Civile, nonché dei reati tributari, in riferimento ai quali si rimanda al paragrafo 7.11 (Area sensibile concernente i reati tributari).

Limitatamente alla gestione dei rapporti con l'outsourcer esterno nell'ambito del presidio della redazione del bilancio della Società, sussiste altresì il rischio della commissione dei reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Si evidenzia che le regole 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 a dare o promettere utilità*", "*Traffico di inlfuenze illecite*", nonché dei reati di "*Riciclaggio*" e "*Autoriciclaggio*".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

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, alla determinazione degli oneri fiscali e allo svolgimento degli adempimenti relativi alle imposte dirette ed indirette. Tali attività attengono ai seguenti processi operativi:

- Gestione della contabilità;
- Gestione del bilancio;
- Gestione degli adempimenti fiscali.

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

I documenti che contengono comunicazioni relative alla situazione economica, patrimoniale e finanziaria della Società sono redatti dal Consulente esterno in base a specifici processi e prassi in essere che:

- identificano con chiarezza e completezza i soggetti interessati, nonché i dati e le notizie che gli stessi devono fornire;
- identificano i criteri per le rilevazioni contabili delle singole operazioni e per 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 ai soggetti responsabili 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 basa sui seguenti fattori:

- Ruoli e responsabilità definiti:
  - il Bilancio è approvato dal Consiglio di Amministrazione della Società;
  - tutti i soggetti di volta in volta interessati della Società e del Consulente esterno sono responsabili dei processi che contribuiscono alla produzione delle voci contabili e/o delle attività valutative ad essi demandate e degli eventuali commenti in bilancio di propria competenza;
  - la decisione in merito al passaggio a perdite è di esclusiva competenza del Consiglio di Amministrazione della Società;
  - il Consulente esterno definisce al proprio interno 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 relative alla situazione economica, patrimoniale e finanziaria della Società prevede il coinvolgimento di distinti soggetti, operanti nelle diverse fasi del processo.

- Attività di controllo:
  - le attività di predisposizione dei documenti che contengono comunicazioni relative alla situazione economica, patrimoniale e finanziaria della Società sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali.

    <u>Principali controlli svolti dal Consulente esterno</u>:
    - 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 i soggetti interessati 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.

    <u>Principali controlli posti in essere dalla Società:</u>
    - 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.

    Inoltre, il Bilancio prodotto dal Consulente esterno è verificato dal Collegio dei Sindaci.

- 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 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, connesse all'attività di chiusura di bilancio, effettuate dai soggetti deputati alla gestione del Bilancio, sono supportate da adeguata documentazione dalla quale sia possibile desumere i criteri adottati e, analiticamente, lo sviluppo dei relativi calcoli;

- tutta la documentazione relativa ai controlli periodici effettuati viene archiviata dai soggetti coinvolti nel processo;
- tutta la documentazione di supporto alla stesura del bilancio è archiviata dai soggetti deputati alla gestione del Bilancio e/o dai soggetti coinvolti nel processo di redazione delle disclosures.

Principi di comportamento

I soggetti, a qualsiasi titolo coinvolti nelle attività di tenuta della contabilità e della successiva predisposizione delle comunicazioni in merito alla situazione economico e patrimoniale della Società (bilancio di esercizio, ecc.), sono tenuti ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia, nonché i contenuti dei contratti che disciplinano le attività in questione, disposizioni 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, i soggetti coinvolti sono tenuti 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 dei relativi contratti, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni, al fine di fornire agli associati ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società.

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

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni, 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;
- promettere o 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) 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, oppure minacciarli di un danno ingiusto per le medesime motivazioni.

I soggetti interessati 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.

7.4 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 ed i reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa[24]

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.

Si rimanda all'Allegato "Elenco Reati", Sezioni III, IV, V, VI e VII per un'illustrazione sintetica di tali categorie di illeciti e delle relative principali fattispecie delittuose.

7.4.2 Attività sensibili

Il rischio che siano posti in essere i reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali e i reati contro la persona riguarda principalmente, nell'ambito dell'attività attualmente svolta dalla Società, la stipula di contratti di compravendita e di locazione di immobili e la gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali.

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 dei contenziosi e degli accordi transattivi;
- "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*" e "Intermediazione illecita e sfruttamento del lavoro", si individua quale attività aziendale sensibile quella connessa alle procedure acquisitive dei beni e dei servizi e degli incarichi professionali.

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:

- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione dei contenziosi e degli accordi transattivi;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del patrimonio immobiliare e del patrimonio culturale.

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 autoriciclaggio" (cfr. "Area sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché 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.

[24] 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.

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. n. 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, i reati di criminalità organizzata, i reati transnazionali, i reati contro la persona ed i reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa") o non presentino le caratteristiche di transnazionalità in precedenza previste[25]. Successivamente, l'art. 25-octies è stato modificato aggiungendovi il reato di autoriciclaggio[26].

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 (Decreto Lgs. 81/2008).

Si rimanda all'Allegato "Elenco Reati", Sezione VIII, per un'illustrazione sintetica delle fattispecie delittuose previste dall'art. 25-octies del Decreto.

7.5.2 Attività sensibili

L'attività sensibile identificata dal Modello nella quale è maggiore il rischio che siano posti in essere i reati di cui alla presente area sensibile, tenuto conto della specifica operatività della Società, è quella connessa alla stipula di contratti di compravendita e di locazione di immobili, nonché alla gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali.

Con particolare riferimento alla prevenzione dei reati di riciclaggio, 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 contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose.

Si evidenzia che 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 (compresa la fattispecie di autoriciclaggio).

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:

[25] 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.

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

- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione del patrimonio immobiliare e del patrimonio culturale.

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

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti, per quanto rileva ai fini del contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose, nella stipula di contratti di compravendita e di locazione di immobili, nella gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali e nella gestione di omaggi.

Ai sensi del D. Lgs. n. 231/2001, i processi in oggetto potrebbero presentare occasioni per la commissione dei reati di "*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del Processo

Ai fini del contrasto al finanziamento del terrorismo e al riciclaggio dei proventi di attività criminose la Società pone in essere attività di prevenzione consistenti in approfondimenti in merito alla conoscenza dei soggetti con cui intende instaurare rapporti contrattuali (es. controparti dei contratti di compravendita di immobili, fornitori).

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante del presente protocollo.

Principi di controllo

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

- Livelli autorizzativi e responsabilità definite:
  - la stipula di contratti di compravendita e locazione e di altri contratti con terze parti prevede specifici meccanismi autorizzativi;
  - gli atti di compravendita della Società devono essere sottoscritti soltanto da soggetti appositamente incaricati, secondo il vigente sistema dei poteri e delle deleghe;
  - il conferimento di incarichi a fornitori di beni e servizi e il perfezionamento dei contratti con gli stessi spettano esclusivamente a soggetti muniti di idonee facoltà in base al vigente sistema dei poteri e delle deleghe, che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i meccanismi autorizzativi sottostanti le procedure acquisitive di beni e servizi;
  - l'eventuale affidamento a terzi – da parte dei fornitori della Società – di attività in sub-appalto, ove non previsto all'interno del contratto stipulato con il fornitore, è subordinato ad un preventivo assenso da parte della Società;
  - la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati in base a criteri individuati nell'ambito della normativa interna, fatte salve esigenze/forniture occasionali. Tali soggetti devono garantire e su richiesta poter documentare anche con riferimento ai subappaltatori da loro incaricati, in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi, il rispetto della disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti.

- 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;
  - ai fini dell'espletamento di determinate attività connesse al processo in oggetto (ad esempio, ricerca di potenziali controparti locatarie, acquirenti, individuazione di fornitori per la realizzazione di interventi manutentivi degli immobili, etc.), la Società si avvale anche di soggetti esterni.

- Attività di controllo:
  - preventivamente alla stipula di contratti di locazione/vendita relativi agli immobili di proprietà della Società, le offerte pervenute dai potenziali locatari/acquirenti sono oggetto di verifica da parte dei soggetti competenti, sulla base di parametri economici, potenziale locatario/acquirente, condizioni di locazione/vendita;
  - attività di identificazione e verifica dei soggetti con cui la Società intende instaurare rapporti contrattuali, attraverso una valutazione di eventuali profili di rischio legati all'esposizione a fenomeni di riciclaggio o di finanziamento del terrorismo che tiene conto, a titolo esemplificativo e non esaustivo, dell'attività svolta da tali soggetti e della principale localizzazione geografica in cui la stessa ha sede, della finalità della stipula del contratto di compravendita o di locazione, etc.;
  - verifica del rispetto dei criteri individuati dalla normativa interna per la scelta dei fornitori e dei professionisti, ivi compreso il controllo a campione del rispetto delle sopra menzionate garanzie circa l'autenticità e la legittima provenienza dei beni forniti;
  - i competenti soggetti della Società sono incaricati del coordinamento dei soggetti esterni che prestano alla Società attività connesse ai processi oggetto del presente protocollo e del monitoraggio circa il rispetto dei livelli di servizio definiti nell'ambito dei contratti stipulati con i soggetti medesimi.

- 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 di volta in volta interessati 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 di contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose;
  - 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;
  - qualora sia previsto il coinvolgimento di soggetti terzi nell'ambito dei processi in oggetto, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto.

Principi di comportamento

I soggetti a qualsiasi titolo coinvolti nelle attività sensibili individuate nell'ambito della "Area sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio", sono tenuti a osservare le modalità esposte nel presente protocollo, le disposizioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico.

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

- instaurare rapporti contrattuali con soggetti relativamente ai quali si sospetta vi sia una relazione con il riciclaggio e/o 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;
- con specifico riferimento alla vendita/locazione di immobili di proprietà della Società, costituire illecitamente provviste di denaro tramite l'incasso di corrispettivi di vendita/canoni di locazione di importo superiore rispetto a quanto contrattualizzato e successivamente impiegare, sostituire o trasferire tali provviste in attività economiche, finanziarie o speculative, in modo da ostacolarne concretamente la 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.

In generale, inoltre, ove non sia chiara la provenienza di denaro, beni o altre utilità oggetto di attività e/o operazioni svolte nell'ambito dell'operatività della Società, nonché in tutti i casi in cui si riscontrino elementi tali da farne sospettare una provenienza delittuosa, tutti i soggetti coinvolti sono tenuti a sospendere immediatamente le attività e/o operazioni interessate, comunicando e rappresentando il fatto ai propri responsabili e a eventuali altri soggetti/strutture/funzioni competenti, affinché siano posti in essere gli approfondimenti e accertamenti necessari.

I soggetti interessati 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 contro il patrimonio culturale

7.6.1 Fattispecie di reato

Premessa

La L. 22 del 9 marzo 2022, in un contesto di revisione normativa previgente ha ricondotto nel Codice Penale reati precedentemente contenuti nel Codice dei Beni culturali (D. Lgs. 42/2004) aggiungendo altresì nuove fattispecie, ed ha introdotto nel D. Lgs. 231/2001 l'articolo 25 septiesdecies "*Delitti contro il patrimonio culturale*" e l'art. 25 duodevicies "*Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici*".

Si rimanda all'Allegato "Elenco Reati", Sezione IX, per un'illustrazione sintetica delle fattispecie delittuose previste dagli artt. 25-septiesdecies e 25-duodevicies del Decreto.

7.6.2 Attività sensibili

Con l'estensione della responsabilità dell'ente anche ai reati contro il patrimonio culturale e paesaggistico, il legislatore ha inteso ampliare la tutela verso il detto patrimonio.

Con riferimento all'operatività della Società il rischio di commissione di detti reati può presentarsi ad esempio nella gestione del proprio patrimonio culturale (e.g. immobili sottoposti a tutela delle Soprintendenza delle Belle Arti), con riguardo, a titolo esemplificativo, allo svolgimento di lavori di manutenzione/ristrutturazioni che ne pregiudichino il valore artistico.

Si rimanda pertanto ai seguenti protocolli:

- Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione del patrimonio immobiliare e del patrimonio culturale;
- Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose.

7.7 Area sensibile concernente i reati in tema di salute e sicurezza sul lavoro

7.7.1 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 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 rimanda all'Allegato "Elenco Reati", Sezione X, per un'illustrazione sintetica delle fattispecie delittuose previste dall'art. 25-septies del Decreto.

7.7.2 Attività sensibili

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

Come già specificato in precedenza, si evidenzia che la Società ha implementato un sistema di prevenzione e protezione dei rischi in materia di salute e sicurezza nei luoghi di lavoro sulla base dei seguenti presupposti:

- il Direttore Operativo della Società è stato nominato quale Datore di lavoro ai sensi del D.Lgs. 81/08;
- Il Direttore Generale del Fondo controllante (Socio unico della Sommariva 14 Srl) viene individuato anche quale Direttore Operativo della controllata Sommariva 14 Srl e per essa le Strutture del Fondo svolgono le attività competenti, ove applicabili. Nell'adunanza del 27 giugno 2023 il Consiglio di Amministrazione del Fondo ha confermato al Direttore Generale anche le nomie di Referente privacy, Responsabile in materia di salute e sicurezza sui luoghi di lavoro ai sensi del D.Lgs. n. 81/2008 e di Delegato in materia ambientale ai sensi del D.Lgs. n. 152/2006;
- Intesa Sanpaolo S.p.A. fornisce gratuitamente alla Società il personale necessario al suo funzionamento;
- Intesa Sanpaolo S.p.A., proprietaria degli immobili, fornisce gratuitamente al Fondo Controllante i locali (immobili o loro porzioni dotati di tutti gli impianti, arredi, corredi, attrezzature e pertinenze idonei all'uso, nonché tutti i servizi necessari alla normale conduzione degli stessi) per lo svolgimento della propria attività, ivi comprese le attività prestate a favore della Società;
- Intesa Sanpaolo S.p.A. presta specifici servizi a favore della Società ai fini del rispetto degli adempimenti previsti dalle disposizioni normative vigenti in materia di salute e sicurezza nei luoghi di lavoro (D.Lgs. 81/08).

Si riporta di seguito il protocollo che detta i principi di controllo e 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, nonchè – stante quanto suesposto – con le misure di prevenzione implementate dalla Banca a presidio dei rischi oggetto del presente protocollo.

Detto protocollo si applica anche a presidio delle attività svolte da Intesa Sanpaolo S.p.A (ovvero da società terze dalla stessa incaricate).

7.7.2.1 Gestione dei rischi in materia di salute e sicurezza sul lavoro

Premessa

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D.Lgs. n. 81/2008 (di seguito Testo Unico).

Si rammenta anzitutto che, ai sensi del Testo Unico compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e compete al Committente la responsabilità e la gestione dei cantieri temporanei o mobili disciplinati dal Titolo IV del Testo Unico nonché compete ad entrambi, per gli ambiti di rispettiva pertinenza, il rispetto degli obblighi relativi all'affidamento di contratti d'appalto, d'opera o di somministrazione previsti dall'art. 26 del medesimo Testo Unico.

In ottemperanza a quanto disposto dalla predetta normativa la Società, di supporto con la Banca, adotta e tiene aggiornato il "Documento di Valutazione dei Rischi", redatto in conformità alla normativa nazionale ed alle linee guida nazionali ed Europee (INAIL, UNI-EN-ISO, Agenzia Europea per la Salute e Sicurezza).

Il Documento di Valutazione dei Rischi individua, entro l'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 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.

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 le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

La Banca ha adottato e mantiene attivo un Sistema di Gestione della Salute e Sicurezza nei luoghi di Lavoro, sottoposto a verifica annuale da parte di un operatore di certificazione internazionale, conforme alle leggi vigenti e al più avanzato standard di riferimento: UNI ISO 45001:2018 e UNI ISO 45003:2021 che, in maniera più specifica, fornisce linee guida per la gestione dei rischi psicosociali. Le modalità e i processi operativi con i quali l'organizzazione risponde ai requisiti dei predetti Standard Internazionali e garantisce l'adempimento di quanto previsto dall'art. 30 – Modelli di organizzazione e di gestione – del Testo Unico sono esplicitate nella normativa aziendale e nel Documento di Valutazione dei Rischi.

Le risorse 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.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

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 sull'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 delle funzioni Tutela Aziendale, Ambiente ed Energia della Banca.

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 compresenza di personale, collaboratori e clienti della Società;
- controllo sul rispetto degli adempimenti contrattuali nell'esecuzione delle attività.

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'ISPESL[27] e prevede le seguenti fasi:

- valutazione preliminare (necessaria/obbligatoria);
- valutazione approfondita (eventuale).

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 della Banca ritenute necessarie in relazione alle caratteristiche della Società, nonché di eventuali consulenze di specialisti esterni.

Le modalità operative di base per la gestione del processo e l'individuazione delle strutture/figure che hanno le responsabilità delle diverse fasi sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante 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 aziendali che rivestono il ruolo rispettivamente di "Datore di Lavoro" e "Committente";
  - 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/Committente, ovvero a cura dei soggetti da costoro 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:
  - i competenti soggetti/unità operative che hanno il compito di realizzare e di gestire gli interventi (di natura immobiliare, informatica, di sicurezza fisica, ovvero attinenti a processi di lavoro e alla gestione del personale), sono distinte e separate dalla struttura alla quale, per legge e/o normativa interna, sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
  - i soggetti 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 o suo delegato al fine di segnalare criticità ed individuare le conseguenti soluzioni.

- Attività di controllo:
  - i competenti soggetti devono 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 rischi sul lavoro. Il piano, in particolare, deve contemplare:

[27] 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.".

- aree e attività aziendali da verificare (tra le quali le attività di natura organizzativa[28], 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;
- la verifica e, qualora non disponibili su siti istituzionali, l'acquisizione di documentazioni e certificazioni obbligatorie di legge (relative ad edifici, impianti, ruoli, incarichi, abilitazioni, del personale e società ecc.) da parte dei competenti soggetti;
- 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;

- i competenti soggetti devono controllare che tutte le misure di prevenzione e protezione programmate siano attuate, assicurando un costante monitoraggio delle situazioni di rischio e dell'avanzamento dei programmi di intervento previsti dagli specifici documenti di valutazione dei rischi. Tali soggetti si avvalgono, laddove occorra, della collaborazione delle strutture della Banca ovvero di società terze dalla stessa incaricate deputate alla gestione del Personale, degli acquisti, della formazione, 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 ove sono presenti lavoratori esposti a rischi specifici ed effettuano a campione sopralluoghi negli altri ambienti;
- figure specialistiche di alta professionalità e con i titoli ed i requisiti previsti dalle norme specifiche preventivamente valutate, contribuiscono alla valutazione ed alla elaborazione di misure di tutela nel caso di rischi in particolare:
  - il Medico Competente Coordinatore: incaricato dal Datore di Lavoro o suo delegato, 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 o suo delegato, 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

[28] Quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.

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 o suo delegato, 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.101/10;
- 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. E' 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.

- i competenti soggetti/unità operative individuati dal Datore di Lavoro/Committente inoltre provvedono alla verifica dell'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare;
- i competenti soggetti/unità operative individuati 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 nomina-

tivo 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;

- i competenti soggetti/unità operative delegati e/o individuati dal Datore di lavoro e dal Committente devono verificare:
  - che per i beni immobili e/o mobili in corso di reimpossessamento o nei casi in cui si venga a conoscenza di circostanziate notizie concernenti eventuali inadempimenti degli obblighi in capo agli utilizzatori in merito al rispetto della normativa su salute e sicurezza, vengano svolte con diligenza e con una adeguata tempistica tutte le azioni correlate, anche di carattere legale, funzionali alla gestione dei rischi in materia di salute e sicurezza;
  - che per i beni immobili e/o mobili ritornati in possesso sia valutata l'esposizione a rischi in materia di salute e sicurezza e sia pianificata e realizzata la loro "messa in sicurezza";
- i competenti soggetti/unità operative individuati dal Datore di Lavoro, 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;
- i competenti soggetti/unità operative individuati 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;
  - ciascuna soggetto di volta in volta interessato, al fine di consentire la ricostruzione delle responsabilità, deve utilizzare idonei sistemi di registrazione dell'avvenuta effettuazione delle attività, ed è responsabile dell'archiviazione e della conservazione dei contratti stipulati nonché di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rischi in materia di sicurezza e salute dei lavoratori nonché della relativa attività di controllo;
  - ciascun soggetto di volta in volta interessato è responsabile altresì dell'acquisizione, della conservazione e dell'archiviazione di documentazioni e certificazioni obbligatorie di legge qualora non disponibili su siti istituzionali, , 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 tutti i soggetti interessati e autorizzati 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

I soggetti a qualsiasi titolo coinvolti 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 e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico.

In particolare, è tenuto - nei rispettivi ambiti - a:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela e valutando la scelta delle attrezzature di lavoro nonché la sistemazione dei luoghi di lavoro;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- astenersi dall'affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità qualificata e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza;
- 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 appalto, d'opera o di fornitura, ad informare le controparti sui rischi specifici dell'ambiente in cui sono destinate ad operare e ad elaborare ed applicare le misure atte a governare in sicurezza le eventuali interferenze fra le imprese, compresi gli eventuali lavoratori autonomi, evidenziando nei contratti per i quali sia prescritto i costi per la sicurezza;
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- curare il rispetto delle normative in tema di salute e sicurezza nei confronti di tutti i lavoratori non dipendenti, con particolare riferimento all'ambito 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. n. 231/2001.

I soggetti interessati 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 informatici e di indebito utilizzo di strumenti di pagamento diversi dai contanti

7.8.1 Fattispecie di reato

Premessa

La legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa, stipulata a Budapest il 23.11.2001, avente l'obiettivo di promovere la cooperazione internazionale tra gli Stati firmatari al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici, specie in considerazione della natura di tali illeciti, che spesso, nelle modalità della loro preparazione o realizzazione, coinvolgono Paesi diversi.

La riforma della disciplina della criminalità informatica è stata realizzata sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti. L'art. 7 della legge ha inoltre aggiunto al D.Lgs. n. 231/2001 l'art. 24-bis, che elenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli Enti.

La citata legge ha modificato anche il codice di procedura penale, e le disposizioni in tema di protezione dei dati personali, essenzialmente al fine di agevolare le indagini sui dati informatici e consentire per determinati periodi la conservazione dei dati relativi al traffico telematico.

Non sono invece state recepite nell'ordinamento italiano le definizioni di "sistema informatico" e di "dato informatico" contenute nella Convenzione di Budapest; tali definizioni, che si riportano qui di seguito, potranno essere prese come riferimento dalla giurisprudenza in materia:

- "sistema informatico": qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati;
- "dato informatico": qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

Il Decreto legislativo 184/2021 ha introdotto nel catalogo dei reati presupposto della responsabilità dell'ente[29] 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 rimanda all'Allegato "Elenco Reati", Sezione XI e XII, per un'illustrazione sintetica delle fattispecie delittuose previste dagli artt. 24-bis e 25-octies.1 del Decreto.

7.8.2 Attività sensibili

Le attività della Società nelle quali possono essere commessi i 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 trattati in modo illecito i dati informatici della Società stessa sono proprie degli esponenti della Società, del Direttore Operativo e del personale che utilizza le tecnologie dell'informazione.

Si rammenta che la Banca mette gratuitamente a disposizione della Società le strutture e le architetture informatiche necessarie per il suo funzionamento.

[29] Cfr art. 25 octies.1 D. Lgs. 231/2001.

Ciò premesso, si evidenzia che la Banca ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alle disposizioni di Vigilanza e alla normativa europea e nazionale in materia di protezione dei dati personali, per prevenire e controllare i rischi in tema di tecnologia dell'informazione (IT) e di Cybersecurity, a tutela del patrimonio informativo.
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 della Società.

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 riportano qui di seguito, i protocolli che dettano i principi di controllo ed i principi di comportamento applicabili alle sopraelencate attività sensibili e che si completano con la normativa interna (ove presente), che regolamenta le attività medesime, nonché con le misure di prevenzione implementate dalla Banca a presidio dei rischi ogetto dei presenti protocolli.

Si evidenzia altresì che nell'ambito dei protocolli che regolano altre attività sensibili quali la "Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali" ed il "Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose" sono previsti alcuni principi di controllo e di comportamento che esplicano la loro efficacia preventiva anche in relazione ai suddetti reati.

7.8.2.1 Gestione e utilizzo dei sistemi informatici e del patrimonio informativo della Società

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione e nell'utilizzo dei sistemi informatici e del patrimonio informativo della Società.

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 della Società nelle attività connesse con il proprio mandato e nelle relazioni con i terzi che accedono al Patrimonio Informativo della Società;
- 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 della Società.

Il protocollo, inoltre, si applica a tutti i sistemi informatici, compresi quelli basati su tecniche di Intelligenza Artificiale; ogni riferimento a sistemi informatici, servizi informatici, software, etc, deve quindi essere inteso come relativo anche ai sistemi basati sull'Intelligenza Artificiale.

Ai sensi del D. Lgs. 231/2001, i processi di gestione e utilizzo dei sistemi informatici e del patrimonio informativo della Società 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 art. 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 protette[30].

Si intende inoltre prevenire il rischio di commissione di delitti contro l'industria e il commercio, con particolare riguardo al delitto di "Illecita concorrenza con minaccia o violenza".

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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'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 di Intesa Sanpaolo S.p.A. 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.

[30] Cfr. "Area sensibile concernente i reati contro l'industria e il commercio, i reati in materia di violazione del diritto d'autore ed i reati doganali".

La Banca e la Società pongono particolare attenzione alle attività di governo e gestione dei sistemi informatici e del patrimonio informativo al fine di assicurare che lo stesso risulti efficace, efficiente e scalabile, soddisfi le esigenze di business, sia allineato all'evoluzione della tecnologia e garantisca la qualità e affidabilità dei servizi ICT.

Sono, inoltre, previste norme e misure di sicurezza organizzative, comportamentali e tecnologiche e attività di controllo finalizzate ad assicurare che la gestione e l'utilizzo dei sistemi informatici e del patrimonio informativo della Società rispettino la normativa vigente.

Di seguito sono riportati i processi in cui si articolano la gestione e l'utilizzo dei sistemi informatici e del patrimonio informativo della Società.

Il processo relativo alla progettazione, sviluppo e attivazione dei servizi ICT si articola nelle seguenti fasi:

- definizione, pianificazione e attuazione della Strategia ICT e la definizione dell'architettura del sistema informativo;
- analisi del rischio;
- analisi e disegno dei sistemi e delle applicazioni;
- sviluppo del software;
- test e collaudo;
- rilascio in produzione;
- gestione delle terze parti ICT;
- esecuzione di controlli di primo livello.

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.

Il processo di gestione della sicurezza informatica si articola nelle seguenti fasi:

- progettazione e realizzazione soluzioni di sicurezza informatica;
- analisi del rischio e definizione dei requisiti di sicurezza informatica;
- gestione accessi;
- gestione architettura di sicurezza informatica;
- esecuzione di follow-up, monitoraggi e analisi post-mortem in ottica di miglioramento continuo;
- esecuzione di controlli di primo livello di sicurezza informatica;
- monitoraggio eventi sicurezza informatica, gestione eventi critici di sicurezza informatica e notifica eventi verso le Autorità;
- cyber intelligence;
- diffusione della cultura di sicurezza informatica;
- gestione delle certificazioni per la sicurezza informatica;
- presidio sicurezza delle terze parti (classificazione e monitoraggio).

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;
- identificazione e registrazione del titolare;
- gestione del certificato (sospensione, riattivazione, revoca, rinnovo e sblocco PIN).

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante 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 di ciascuna fase operativa caratteristica dei processi sopra descritti. In particolare:
  - la gestione delle abilitazioni avviene tramite la definizione di "profili di accesso" in ragione delle funzioni svolte all'interno della Società;
  - le variazioni al contenuto dei profili sono eseguite dai soggetti deputati al presidio della sicurezza informatica, su richiesta dei soggetti interessati. I soggetti deputati devono 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;
  - le modifiche al sistema informatico devono essere autorizzate in base alla relativa rilevanza secondo quanto previsto dalle normative interne.

- Segregazione dei compiti:
  - sono assegnati ruoli e responsabilità di gestione della sicurezza informatica; 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 della Società;
    - sono attribuite precise responsabilità per la gestione degli aspetti di sicurezza ai soggetti competenti che sviluppano e gestiscono sistemi informatici;
    - sono definite le responsabilità ed i meccanismi atti a garantire la gestione di eventi di sicurezza anomali, delle situazioni di emergenza e crisi;
    - sono attribuite precise responsabilità della predisposizione, validazione, emanazione e aggiornamento delle norme di sicurezza a strutture distinte da quelle incaricate della gestione;
  - le attività di implementazione e modifica dei software, gestione delle procedure informatiche, progettazione, realizzazione e gestione delle soluzioni applicative e delle infrastrutture tecnologiche della Società, controllo degli accessi fisici, informatici e della sicurezza informatica del software sono organizzativamente demandate a soggetti differenti rispetto agli utenti, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informatici;

- 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 informatici e del patrimonio informativo della Società 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.I controlli previsti si basano sulla definizione di specifiche attività finalizzate alla gestione nel tempo anche degli aspetti inerenti alla protezione del patrimonio informativo della Società, quali:
  - la definizione degli obiettivi e delle strategie di sicurezza informatica;
  - la definizione di una metodologia di analisi dei rischi ICT e di sicurezza 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 e dei fornitori 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 delle norme di sicurezza e ICT definite.

  Le principali attività di controllo, tempo per tempo effettuate, e specificamente dettagliate nella normativa interna di riferimento, sono le seguenti.

  Con riferimento alla sicurezza informatica:
  - identificazione e autenticazione dei codici identificativi degli utenti;
  - autorizzazione relativa agli accessi alle informazioni richiesti;
  - controlli di primo livello (ad es., alert management delle soluzioni di antivirus, intrusion detection system, firewalling, patch management, identity and access management, real time monitoring, abuse desk, ecc.), nonché procedure di verifica e reporting (ad es., vulnerability assessment, technical security reporting, ecc.);
  - previsione di tecniche crittografiche e di firma digitale per garantire la riservatezza, l'integrità e il non ripudio delle informazioni archiviate o trasmesse;
  - verifica nel continuo delle misure di sicurezza informatica applicate.

  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;
  - previsione di specifiche procedure (test management) volte ad assicurare che i prodotti software, i servizi ICT e le misure di sicurezza dell'informazione soddisfino i requisiti specificati, che siano adatti al loro scopo.

  Con riferimento ai sistemi di Intelligenza Artificiale, in aggiunta alle altre attività di controllo:

- previsione di adeguati controlli, in particolare per l'Intelligenza artificiale generativa[31], al fine di assicurare la loro corretta classificazione e, per i sistemi classificati ad alto rischio, garantire il rispetto delle regole di fairness, di sorveglianza umana, e di trasparenza e spiegabilità.

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 manutenuti 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 rimuovibili 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 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 gestione degli incidenti di sicurezza:

- previsione di opportuni processi per la 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, prevenire il ripetersi di comportamenti inadeguati e attivare l'eventuale escalation che può condurre anche all'apertura di uno stato di emergenza o crisi.

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

[31] Tecnologie di Intelligenza artificiale in grado di generare contenuti di testo, immagini, video, musica o altro in risposta a un input utente).

- 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);
- lo sviluppo, l'implementazione, il funzionamento e/o la configurazione del sistema informatico devono essere adeguatamente documentati anche al fine di spiegarne il funzionamento e le interdipendenze;
- 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, i soggetti di volta in volta interessati sono responsabili dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.

Principi di comportamento

I soggetti a qualsiasi titolo coinvolti nelle attività di gestione e utilizzo di sistemi informatici e del patrimonio informativo della Società sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico.

In particolare:

- la Società deve tenere un inventario aggiornato delle risorse ICT (compresi i sistemi ICT, i dispositivi di rete, le banche dati, ecc.) e delle relative dipendenze da altri sistemi e processi interni ed esterni; in tale contesto sono individuati e censiti anche i sistemi informatici basati su tecniche di Intelligenza Artificiale e gli applicativi che si connettono con la Pubblica Amministrazione o con le Autorità di Vigilanza;
- i soggetti coinvolti nel processo accedono in base ai "profili di accesso" definiti in ragione delle funzioni svolte all'interno della Società;
- le attività di sviluppo e di test di componenti del sistema informatico della Società devono essere effettuate in ambienti separati da quelli di produzione;
- il passaggio in produzione di nuove componenti del sistema informatico della Società o di modifiche di componenti esistenti deve essere preceduto da test che ne certifichino il corretto funzionamento, la rispondenza ai requisiti iniziali, l'assenza di difetti che possano compromettere la sicurezza del sistema informatico della Società o di quelli di terzi;
- il personale/ogni amministratore del sistema è tenuto a segnalare alle funzioni competenti 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 emergenza o 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 nella gestione dei sistemi informatici e del patrimonio informativo della Società nonché nell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, deve essere assicurato che tali soggetti possiedano appropriate competenze tecniche, rispondano ad adeguati standard di sicurezza informatica e continuità operativa e non presentino problemi di natura economico-

patrimoniale; 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 dal Direttore Operativo della Società; 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 della Banca, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- acquisire e/o trattare dati e informazioni e/o creare banche dati/liste che non siano necessari e direttamente pertinenti allo svolgimento della propria funzione, a prescindere dalla possibilità di accedere agli applicativi di riferimento;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, troian, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ovvero ostacolare il funzionamento dei sistemi informatici o telematici di pubblico interesse;
- 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 informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero favorirne l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- costringere taluno a fare o ad omettere qualche cosa attraverso l'utilizzo o la minaccia di utilizzo illecito di sistemi informatici o telematici della Società, al fine di procurare a sé o ad altri un ingiusto profitto con altrui danno;
- 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 e/o tramite l'utilizzo di sistemi di Intelligenza Artificiale condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:
  - diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;

- abusivamente duplicare, detenere o diffondere in qualsiasi forma programmi per elaboratore od opere audiovisive o letterarie;
- detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;
- riprodurre banche di dati su supporti non contrassegnati dalla SIAE, diffonderle in qualsiasi forma senza l'autorizzazione del titolare del diritto d'autore o in violazione del divieto imposto dal costitutore;
- rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;
- importare, promuovere, installare, porre in vendita, modificare o utilizzare, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente;
- sviluppare o addestrare sistemi di Intelligenza Artificiale, in particolare Generativa, senza rispettare la normativa in materia di dati personali o in violazione della normativa in materia di diritto d'autore.

I soggetti interessati 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.

7.8.2.2 Gestione e utilizzo degli strumenti di pagamento diversi dai contanti

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione e nell'utilizzo degli strumenti di pagamento diversi dai contanti.

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.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del Processo

Il processo di gestione e utilizzo degli strumenti di pagamento diversi dai contanti si articola nei seguenti processi:

- Gestione delle carte di pagamento (carte di debito e di servizio, carte di credito, carte prepagate);
- Gestione di incassi e pagamenti (es., per quanto applicabile, assegni, bonifici, addebiti diretti, RIBA – MAV – effetti);
- Gestione dei Canali Digitali di incasso e pagamento (accesso e utilizzo del remote banking);
- Gestione delle risorse Umane con riferimento alle carte di credito aziendali, ai buoni pasto, alle carte di servizio per le autovetture (carta carburante, telepass) rilasciate al personale.

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante 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 Direttore Operativo della Società tramite delega interna;
  - sono identificati meccanismi di autenticazione basati sul rischio delle operazioni relativi a strumenti di pagamento diversi dai contanti.

- Segregazione dei compiti:
  - sono attribuite precise responsabilità nella gestione del processo di gestione:
    - delle carte di pagamento attraverso la definizione di compiti e controlli specifici in merito alle attività di richiesta, consegna, sostituzione, rinnovo, attivazione, revoca, rinuncia o recesso del dipendente;
    - degli assegni (richiesta e ottenimento, gestione degli adempimenti in caso di smarrimento, sottrazione e distruzione degli stessi);
    - dei canali digitali (richiesta attivazione del servizio, gestione delle credenziali).

- 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:
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, i soggetti di volta in volta interessati 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

I soggetti a qualsiasi titolo coinvolti nelle attività di gestione e di utilizzo degli strumenti di pagamento diversi dai contanti sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico.

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;
- il personale deve segnalare immediatamente al Direttore Operativo della Società qualunque tentativo di falsificazione ed indebito utilizzo di strumenti finanziari diversi dai contanti del quale venga a conoscenza. Il Direttore Operativo della Società a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso.

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 soggetti interessati 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.

7.9 Area sensibile concernente i reati contro l'industria e il commercio, i reati in materia di violazione del diritto d'autore ed i reati doganali

7.9.1 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. n. 231/2001, gli artt. 25-bis e 25-bis.1 richiamano fattispecie previste dal codice penale in tema di industria e di commercio[32], mentre l'art. 25-novies – al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno[33] 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 contrabbando, introdotti nell'articolo 25- sexiesdecies[34] al fine di recepire le disposizioni della legislazione europea poste a tutela degli interessi della finanza pubblica dell'Unione europea[35].

Si rimanda all'Allegato "Elenco Reati", Sezioni XIII, XIV e XV per un'illustrazione sintetica delle fattispecie delittuose previste dagli artt. 25-bis, 25-bis.1, 25-novies e 25-sexiesdecies del Decreto.

7.9.2 Attività 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'eventuale approvvigionamento o nell'utilizzo di prodotti, software, banche dati ed altre opere dell'ingegno.

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:

- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;
- Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo della Società.

Relativamente ai reati di contrabbando, i rischi di commissione dei medesimi possono presentarsi nei processi relativi alle procedure acquisitive di beni oggetto d'importazione, nonché a carattere più generale negli adempimenti da porre in essere nei confronti dell'Amministrazione doganale.

Si rimanda pertanto al seguente protocollo:

- Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali;

che contiene principi di controllo e di comportamento che esplicano la loro efficacia preventiva anche in relazione ai reati suddetti.

[32] A seguito della modifica apportata dalla L. 99/2009, l'art. 2 *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 c.p., i quali hanno in comune con i primi il bene giuridico principalmente tutelato e cioè la fede pubblica, intesa quale affidamento che la generalità dei cittadini ripone nella veridicità di determinati oggetti, segni o attestazioni.

[33] 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.

[34] Cfr. l'articolo 5 del D. Lgs. 75/2020.

[35] La possibilità di commissione dei reati doganali, tenuto conto dell'operatività della Società, è stata ritenuta ragionevolmente remota o non applicabile.

7.10 Area sensibile concernente i reati ambientali

7.10.1 Fattispecie di reato

Premessa

L'art. 25-undecies del D.Lgs. n. 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 enti[36].
Si tratta di reati descritti nel codice penale, nel D.Lgs. n. 152/2006 (Codice dell"ambiente, per brevità nel seguito C. A.) e in varie leggi speciali, sia di natura delittuosa sia di tipo contravvenzionale[37].

Si rimanda all'Allegato "Elenco Reati", Sezione XVI, per un'illustrazione sintetica delle fattispecie delittuose previste dall'art. 25-undecies del Decreto.

7.10.2 Attività sensibili

Con riferimento all'operatività della Società, i rischi di commissione dei reati ambientali possono presentarsi più verosimilmente nei processi relativi agli immobili di proprietà della Società (in termini di gestione e manutenzione degli stessi), nella gestione degli adempimenti legislativi previsti in materia di smaltimento di rifiuti (con riferimento alla produzione di rifiuti presso i fabbricati), nonché nella selezione dei fornitori (con particolare riferimento agli interventi di manutenzione).
Con riferimento alla gestione degli adempimenti legislativi in materia di smaltimento di rifiuti prodotti presso la sede della Società, messa a disposizione da Intesa Sanpaolo S.p.A, i connessi adempimenti in materia ambientale ricadono sotto la responsabilità della Banca stessa, la quale ha provveduto ad implementare idonee misure di prevenzione atte a prevenire i suddetti reati.
Di norma tutti i processi relativi alla gestione ordinaria e straodinaria degli immobili di proprietà è effettuata con il supporto di strutture di Intesa Sanpaolo, seguendo protocolli operativi previsti dal Modello di organizzazione, gestione e controllo di quest'ultima.

Si riporta di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia ambientale nell'ipotesi, finora non ancora verificatesi, che i processi siano gestiti con altri fornitori di servizi. In tale circostanza si fa riferimento ai seguenti altri protocolli del Modello atti a prevenire la commissione dei reati di cui al presente Capitolo:

- *"Gestione delle attività inerenti la richiesta di autorizzazioni o l'esecuzione di adempimenti verso la Pubblica Amministrazione"*;
- *"Gestione delle procedure acquisitive dei beni e dei servizi e degli incarichi professionali"*.

[36] L'art. 25-undeciesdel D. Lgs. 231/2001, in vigore dal 16 agosto 2011, nel testo dapprima inserito dal D. Lgs. 121/11, 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.
[37] Le fattispecie delittuose sono quelle previste dal C.A. agli artt. 258, comma 4, 260, c. 1 e 2, 260-bis, commi 6, 7e 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.

7.10.2.1 Gestione dei rischi in materia ambientale

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione dei rishci in materia ambientale.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

Descrizione del processo

Ai fini del presidio dei rischi in materia ambientale si rimanda ai seguenti processi:

Gestione immobiliare della Società:

- gestione e manutenzione degli immobili sul territorio;
- pianificazione lavori;
- esecuzione lavori.

Gestione degli adempimenti legislativi in tema di rifiuti:

- smaltimento dei rifiuti concernenti gli immobili di proprietà della Società;
- prodotti presso la sede della Società (rientranti nei processi e protocolli di controllo di Intesa Sanpaolo).

Gestione della spesa e degli acquisti:

- selezione dei fornitori (con particolare riferimento ai fornitori incaricati degli interventi - di manutenzione sugli immobili di proprietà della Società e smaltimento rifiuti).

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrante 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:
  - il conferimento dell'incarico ed il perfezionamento del contratto 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. L'approvazione della richiesta d'acquisto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere, nonché alla Banca per le spese oggetto di refusione da parte della stessa. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
  - ogni trasporto di rifiuti speciali deve essere accompagnato da un formulario d'identificazione sottoscritto dal trasportatore e controfirmato dal destinatario (soggetto autorizzato al recupero o smaltimento); nel caso di contratti stipulati da parte della Società con ditte incaricate esclusivamente dello smaltimento dei materiali in relazione alle manutenzioni di immobili di proprietà della Società, il formulario è debitamente acquisito da parte della Società;
  - 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 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:
  - i soggetti interni o esterni alla Società, che hanno il compito di realizzare e di gestire gli interventi quali servizi alla persona, servizi agli edifici, manutenzioni edili, opere edilizie/impiantistiche ed altri servizi integrati (es.: fornitura toner, ricariche per impianti di refrigerazione e condizionamento, ecc.) sono distinti e separati dai soggetti, interni o esterni alla Società, ai quali sono attribuiti compiti di consulenza in tema di valutazione dei rischi ambientali e di controllo sulle misure atte a prevenirli e a ridurli;
  - in presenza di situazioni di smaltimento di rifiuti senza la presenza di funzionari dell'Agenzia delle Entrate, la Società si avvale del Notaio per la redazione del verbale di consegna dei rifiuti stessi.
- Attività di controllo:
  - il formulario d'identificazione dei rifiuti speciali compilato e sottoscritto dal trasportatore deve essere verificato dal soggetto incaricato;
  - verifica a campione sulla corretta gestione dei rifiuti con particolare riguardo a quelli speciali e, se presenti, a quelli pericolosi da parte dei soggetti competenti;
  - verifica sulla corretta gestione da parte dell'appaltatore dei rifiuti derivanti dalle attività di manutenzione ordinaria e straordinaria e da ristrutturazioni immobiliari degli immobili della Società. In particolare l'appaltatore è tenuto a ritirare a propria cura gli "scarti" dal proprio ciclo di lavoro e i soggetti (anche esterni) all'uopo incaricati della Società 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' Edifici, Servizi alle Persone, ecc.) degli immobili di proprietà della Società, con particolare riguardo alla regolare tenuta dei libretti degli impianti delle caldaie e gruppi frigoriferi nonché ai report manutentivi periodici redatti dai fornitori che hanno in appalto i servizi suddetti.
- 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 inerente ai processi con particolare riferimento alla manutenzione di impianti (quali ad esempio controlli in merito alla corretta tenuta e conservazione dei libretti degli impianti delle caldaie e dei gruppi frigoriferi secondo quanto previsto dalla normativa vigente, specie relativamente alle loro emissioni);
  - con riferimento alle autorizzazioni richieste ai fornitori che si occupano del recupero e smaltimento dei rifiuti è prevista l'archiviazione di copia della documentazione necessaria per la prestazione del servizio nel rispetto dei requisiti regolamentari definiti (ad es., attestazione circa il possesso delle autorizzazioni/certificazioni richieste dalla normativa di settore per lo svolgimento dell'attività, polizze assicurative aggiornate, lista del personale addetto alle manutenzioni aggiornata, ecc.);
  - 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;
  - fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, tutti i soggetti coinvolti 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

I soggetti, a qualsiasi titolo coinvolti nella gestione dei rischi in materia ambientale, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge e l'eventuale normativa interna esistenti in materia, nonché le previsioni del Codice Etico.

In particolare, tutti i soggetti che operano per la Società sono tenuti – nei rispettivi ambiti - 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 eventuali 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. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico;
- 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. n. 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.: materiali per gli impianti di refrigerazione, fornitura toner ecc.) specifiche clausole sul rispetto della normativa ambientale;
- 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;
- osservare le disposizioni di legge, la normativa interna e dalle Autorità competenti;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, qualsiasi situazione di emergenza ambientale di cui si dovesse venire a conoscenza (es. gravi malfunzionamenti degli impianti).

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- depositare i rifiuti al di fuori dal "Deposito Temporaneo Rifiuti" e consegnare i rifiuti speciali a fornitori incaricati del trasporto non in possesso delle necessarie autorizzazioni.

I soggetti interessati 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.

7.11 Area sensibile concernente i reati tributari

7.11.1 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)[38].

Si rimanda all'Allegato "Elenco Reati", Sezione XVIII, per un'illustrazione sintetica delle fattispecie delittuose previste dall'art. 25- quinquiesdecies del Decreto.

7.11.2 Attività sensibili

Il rischio di commissione dei reati tributari può presentarsi nell'attività della Società. Esso è specificamente presidiato dal protocollo "Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari" esposto al successivo punto.

Per quanto riguarda i rapporti con i terzi, quali aderenti, fornitori di servizi e controparti in genere al fine di mitigare il rischio di essere coinvolta in illeciti fiscali dei medesimi, la Società dispone di una normativa interna relativa a:

- procedura per il pagamento delle fatture;
- procedura di liquidazione delle commissioni di gestione.

Che contengono principi di controllo e di comportamento da rispettare anche ai fini della prevenzione dei reati fiscali.

[38] La disciplina dei reati tributari è stata riformata dal D. L. 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. 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.74/2000 - anche i reati dichiarativi di cui agli articoli 2, 3 e 4 solo tentati, con effetto dal 30 luglio 2020.

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

Premessa

Il presente protocollo si applica a tutti i soggetti coinvolti nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari.

Ai sensi del D. Lgs. n. 231/2001, il processo potrebbe presentare occasioni per la commissione dei seguenti reati tributari: "*Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti*", "*Dichiarazione fraudolenta mediante altri artifici*", "*Emissione di fatture o altri documenti per operazioni inesistenti*", "*Occultamento o distruzione di documenti contabili*" e di "*Sottrazione fraudolenta al pagamento di imposte*".

La società intende mantenere un rapporto collaborativo e trasparente con l'Autorità.

Si rileva come i principi di controllo e di comportamento definiti nell'ambito del presente protocollo risultano applicati anche a presidio delle attività esternalizzate sia presso società del gruppo Intesa Sanpaolo sia presso outsourcer esterni, sulla scorta delle relative convenzioni/contratti con gli stessi.

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.

Ai sistemi informatici che supportano i processi indicati nel presente protocollo si applicano i principi di controllo e di comportamento previsti dal protocollo "*Gestione e utilizzo dei sistemi informatici e del patrimonio informativo di Gruppo*".

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 che riguardano:

- le fasi di acquisto di beni e servizi;
- la rappresentazione dei fatti di gestione nella contabilità e nei sistemi aziendali;
- la gestione degli adempimenti connessi alla fatturazione passiva;
- la predisposizione delle dichiarazioni fiscali e la corretta liquidazione/riversamento delle relative imposte.

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

Le modalità operative di base per la gestione del processo sono disciplinate in parte nell'ambito della normativa interna, sviluppata ed aggiornata a cura dei soggetti competenti, che costituisce parte integrantedel 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 dal funzionigramma/mansionario ovvero Direttore Operativo;
  - 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 dalla Società e sotto il controllo del Direttore Operativo e/o degli eventuali soggetti dal medesimo appositamente incaricati;

- ogni accordo/convenzione con l'Agenzia delle Entrate è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
- nei casi in cui l'orientamento fiscale che la società intende adottare non dovesse essere condiviso dall'Agenzia delle Entrate, la sua definitiva adozione deve essere approvata dal Consiglio di Amministrazione, previa valutazione del Direttore Operativo in ordine ai rischi e ai costi/benefici derivanti dalla posizione che si intende assumere e acquisizione del parere di almeno un autorevole consulente fiscale esterno.

- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi di gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari. In particolare:
  - le attività di cui alle diverse fasi del processo devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.
- Attività di controllo:
  - controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle autorità fiscali da parte dei soggetti interessati 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, i soggetti di volta in volta interessati sono responsabili dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.

Principi di comportamento

I soggeti a qualsiasi titolo coinvolti nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari oggetto del, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge e la normativa interna esistenti in materia, nonché le eventuali previsioni del Codice Etico.

In particolare, tutti i soggetti che svolgono operazioni per conto della società sono tenuti – nei rispettivi ambiti - a:

- garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari dela 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 della società;

- agire secondo i valori dell'onestà e dell'integrità nella gestione della variabile fiscale, nella consapevolezza che il gettito derivante dai tributi costituisce una delle principali fonti di contribuzione allo sviluppo economico e sociale dei Paesi in cui opera;
- garantire la diffusione di una cultura aziendale improntata ai valori di onestà e integrità e al principio di legalità;
- mantenere un rapporto collaborativo e trasparente con l'Autorità Fiscale garantendo a quest'ultima, tra l'altro, la piena comprensione dei fatti sottesi all'applicazione delle norme fiscali;
- eseguire gli adempimenti fiscali nei tempi e nei modi definiti dalla normativa o dall'autorità fiscale;
- evitare forme di pianificazione fiscale che possano essere giudicate aggressive da parte delle autorità fiscali;
- interpretare le norme in modo conforme al loro spirito e al loro scopo rifuggendo da strumentalizzazioni della loro formulazione letterale;
- rappresentare gli atti, i fatti e i negozi intrapresi in modo da rendere applicabili forme di imposizione fiscale conformi alla reale sostanza economica delle operazioni;
- garantire trasparenza alla propria operatività e alla determinazione dei propri redditi e patrimoni evitando l'utilizzo di strutture, anche di natura societaria, che possano occultare l'effettivo beneficiario dei flussi reddituali o il detentore finale dei beni;
- rispettare le diposizioni atte a garantire idonei prezzi di trasferimento per le operazioni "infragruppo" con la finalità di allocare, in modo conforme alla legge, i redditi generati;
- collaborare con le autorità competenti per fornire in modo veritiero e completo le informazioni necessarie per l'adempimento e il controllo degli obblighi fiscali;
- rapportarsi con le amministrazioni fiscali, ispirandosi alla trasparenza e fiducia reciproca e nell'obiettivo di prevenire i conflitti, riducendo quindi la possibilità di controversie;
- proporre alla clientela prodotti e servizi che non consentano di conseguire indebiti vantaggi fiscali non altrimenti ottenibili, prevedendo inoltre idonee forme di presidio per evitare il coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela.

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

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità Fiscali in errore;
- procedere con il pagamento di una fattura senza verificare preventivamente l'effettività, la qualità, la congruità e tempestività della prestazione ricevuta e l'adempimento di tutte le obbligazioni assunte dalla controparte;
- utilizzare strutture o società artificiose al solo fine di eludere la normativa fiscale;
- rilasciare documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- occultare scritture contabili o altri documenti di cui è obbligatoria la conservazione;
- 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 fittizia-

mente 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 soggetti interessati 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.