MODELLO ORGANIZZATIVO AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

di PKB Private Bank S.A.

15.03.2023

INDICE

PARTE GENERALE

1. Premessa

Ai sensi della normativa italiana, il Decreto Legislativo 8 giugno, n. 231 (il "**D.Lgs. 231/2001**" o il "**Decreto**") ha introdotto la disciplina della responsabilità amministrativa degli enti (nozione che comprende gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica) per gli illeciti amministrativi dipendenti da reato.

Detta disciplina prevede una responsabilità diretta dell'ente - con conseguente soggezione di quest'ultimo a sanzioni patrimoniali e interdittive - per la commissione o il tentativo di commissione di taluni reati tassativamente elencati (i c.d. reati presupposto), il cui elenco si è progressivamente esteso nel tempo, nell'interesse o a vantaggio dell'ente medesimo, da parte di soggetti allo stesso funzionalmente legati, siano essi:

(i) 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 (i "**Soggetti Apicali**"); ovvero
(ii) persone fisiche sottoposte alla direzione o alla vigilanza di uno dei Soggetti Apicali (i "**Soggetti Vigilati**").

La responsabilità prevista a carico degli enti si aggiunge, e non si sostituisce, alla responsabilità penale personale della persona fisica che sia materialmente l'autrice del reato. La responsabilità amministrativa degli enti sussiste anche se l'autore del reato non è stato identificato e ancorché il reato si sia estinto nei confronti del reo per una causa diversa dall'amnistia.

Per i reati commessi dai Soggetti Apicali, il Decreto introduce una sorta di *"presunzione relativa*" di responsabilità dell'ente, dal momento che si prevede l'esclusione della sua responsabilità solo se esso dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo dotato di autonomi poteri di iniziativa e di controllo.

Per i reati commessi da Soggetti Vigilati, l'ente può essere chiamato a rispondere solo qualora si accerti che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. In questa ipotesi, il Decreto riconduce la responsabilità ad un inadempimento dei doveri di direzione e di vigilanza, che gravano tipicamente sul vertice aziendale (o sui soggetti da questo delegati). L'inosservanza degli obblighi di direzione o vigilanza non ricorre se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

In ogni caso, sia che il reato sia stato commesso da un Soggetto Apicale o da un Soggetto Vigilato, l'ente non risponde, per espressa previsione legislativa (art. 5, co. 2, D.Lgs. 231/2001), se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.

Come evidenziato sopra, l'art. 6 del D.Lgs. 231/2001 introduce una particolare forma di esonero dalla responsabilità in oggetto qualora l'ente dimostri, in particolare, di aver adottato ed efficacemente attuato attraverso il suo organo dirigente, prima della commissione del reato, un modello idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto prevede, inoltre, che – in relazione all'estensione dei poteri delegati ed al rischio di commissione dei reati presupposto – il modello debba rispondere alle seguenti esigenze:

a) individuare le aree a rischio di commissione dei reati previsti dal Decreto;
b) prevedere specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
e) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

L'art. 7 del D.Lgs. 231/2001 specifica, inoltre, che il modello deve prevedere - in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta - misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

IL D.Lgs. 231/2001 prevede, infine, che a seguito dell'adozione del modello, quest'ultimo debba essere anche efficacemente attuato, tramite:

a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nello stesso modello.

2. Il Modello della Banca

2.1. La Banca

PKB Private Bank SA (la "**Banca**") è una banca di diritto svizzero, con sede in Lugano (Svizzera), capogruppo del Gruppo Bancario PKB (il "**Gruppo**"), avente società operanti a livello internazionale. Fanno parte del Gruppo anche società di diritto italiano, ossia Cassa Lombarda S.p.A., banca di diritto italiano che offre servizi di *private banking* e *wealth management*, e PKB Servizi Fiduciari S.p.A., fiduciaria statica di diritto italiano che offre servizi di amministrazione fiduciaria di beni per conto di terzi.

La Banca è specializzata nella prestazione in Svizzera dell'attività di *private banking*, nonché, in un'ottica di maggiore attrattività per la clientela target (Svizzera ed internazionale), di servizi complementari di credito, principalmente ipotecari e garantiti da valori mobiliari. La Banca offre anche in maniera opportunistica servizi alla clientela "corporate banking", ovvero imprese con esigenze di cash management, finanziamento di varia natura, nonché consulenza legata alla gestione della liquidità.

Per quanto riguarda l'operatività con clientela italiana, la Banca è autorizzata da Banca d'Italia (autorizzazione rilasciata in data 27 dicembre 2011), ai sensi dell'art. 16 comma 4 del D. Lgs 385/93 ("**TUB**"), a prestare in Italia, senza stabilimento di succursali, i seguenti servizi bancari:

a) raccolta di depositi o di altri fondi con obbligo di restituzione;
b) operazioni di prestito (compresi in particolare mutui, linee di credito ad aziende, prestiti c.d. "Lombard Loan");
c) rilascio di garanzie e di impegni di firma;
d) consulenza alle imprese in materia di struttura finanziaria, di strategia industriale e di questioni connesse, nonché consulenza e servizi nel campo delle concentrazioni e del rilievo di imprese;
e) servizi di intermediazione finanziaria del tipo "money broking" (ossia, intermediazione in cambi senza assunzione di rischi in proprio);
f) custodia e amministrazione di valori mobiliari;
g) locazione di cassette di sicurezza.

La suddetta autorizzazione *ex* art. 16, co. 4, del Testo Unico Bancario non consente in alcun modo lo svolgimento in Italia di servizi di investimento (secondo la definizione contenuta nella Direttiva UE 2014/65 sui mercati degli strumenti finanziari, c.d. "**MiFID II**"), quali, a titolo esemplificativo e non esaustivo, la conclusione di mandati di gestione patrimoniale, consulenza in materia di investimenti o mera esecuzione di ordini. Alla Banca è, tuttavia, consentito prestare i suddetti servizi di investimento a favore di clienti italiani esclusivamente nei casi di iniziativa autonoma da parte degli stessi e in assenza di qualsivoglia sollecitazione o promozione da parte della Banca (c.d. regime di *reverse solicitation* di cui all'art. 42 della MIFID II).

Coerentemente con il proprio regime autorizzativo, la Banca non dispone di alcuna stabile organizzazione in Italia e opera, tramite i Soggetti Apicali e i Soggetti Vigilati, quasi esclusivamente dalla Svizzera.

Al fine di svolgere l'attività transfrontaliera con la clientela privata e/o commerciale nel rispetto del diritto estero (in particolare, quello italiano) ed evitare rischi di *compliance*, giuridici e di responsabilità con le Autorità estere (in particolare, quelle italiane) nonché tutelare la reputazione della Banca, quest'ultima ha adottato una specifica Norma Operativa ("*Attività transfrontaliera – cross border*") che disciplina le attività *cross-border*. A tale Norma Operativa sono allegate

specifiche istruzioni operative per ciascun paese in cui la Banca svolge attività *cross-border*, tra cui l'Italia ("*Manuale Paese Italia*"). Il corpus normativo interno in materia di attività transfrontaliera prevede nello specifico i seguenti presidi:

1. l'identificazione, in modo dettagliato, delle attività bancarie consentite e non consentite a favore della clientela residente in Italia, tenuto conto del regime autorizzativo della Banca e delle disposizioni normative e regolamentari applicabili;
2. la formazione del personale a contatto con la clientela residente in Italia e controlli specifici sull'adempimento degli obblighi formativi;
3. un processo autorizzativo di ciascun viaggio all'estero (i.e. in Italia);
4. la predisposizione di specifici rapporti sui viaggi effettuati in Italia (c.d. "*Trip Report*"), la registrazione degli stessi nel data base informatico e controlli trimestrali sui medesimi da parte della funzione Legal & Compliance, con conseguente processo di segnalazione di eventuali anomalie riscontrate alle funzioni e organi competenti (i.e. Responsabile della Funzione Legal & Compliance, al CRO e ai Capi Divisione 1 e 2);
5. uno specifico processo di documentazione della "*reverse solicitation*" da parte del cliente, al fine di consentire l'accertamento del carattere genuino dell'iniziativa del cliente, senza alcun invito o comunicazione da parte della Banca. Anche tale processo è soggetto a controlli periodici da parte della funzione Legal e Compliance;
6. l'attribuzione al Comitato Rischi del compito di seguire costantemente l'evoluzione del quadro normativo applicabile ai paesi esteri in cui la Banca svolge attività *cross-border* (tra cui l'Italia), valutare i relativi rischi e, quindi l'aggiornamento del Manuale Paese (Italia).

2.2. Il Modello

Il Modello è stato predisposto considerando i reati presupposto e gli illeciti amministrativi, previsti ai sensi del Decreto, che assumono rilievo per la Banca in ragione della sua concreta operatività nei confronti della clientela residente in Italia e/o di attività rilevanti in termini di applicabilità del quadro normativo italiano di riferimento (di seguito i reati presupposto e gli illeciti amministrativi ai sensi del Decreto contemplati dal presente Modello, come anche descritti nella Parte Speciale del Modello, gli "**Illeciti Rilevanti**").

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 Banca, in quanto idonei a valere anche come misure di prevenzione di reati e di comportamenti illeciti in genere, inclusi gli Illeciti Rilevanti (si veda la Sezione 2.7 seguente).

Nel corso della predisposizione del Modello, inoltre, sono state condotte interviste con il *management* della Banca al fine di discutere e valutare la concreta esposizione della Banca stessa al rischio di commissione degli Illeciti Rilevanti nonché individuare e meglio specificare i presidi procedurali già in essere.

Nella predisposizione del presente Modello, inoltre, la Banca si è ispirata alle linee guida emanate dall'Associazione Bancaria Italiana (le "**Linee Guida ABI**").

2.3. Ambito di applicazione territoriale della normativa penale italiana

Ai fini della lettura del presente Modello, è importante considerare che il codice penale italiano disciplina in via generale i criteri di applicazione territoriale della normativa penale, che trovano applicazione fatte salve le previsioni dettate con riferimento a specifiche fattispecie. In particolare, ai sensi dell'art. 6 c.p. si prevede che:

- è punito secondo la legge italiana chiunque commette un reato nel territorio dello Stato; e
- un reato si considera commesso nel territorio dello Stato, "quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".

Ai sensi del codice penale italiano (artt. 7-10 c.p.), così come anche della normativa speciale relativamente a specifiche fattispecie, vi sono casi in cui si prevede l'imputabilità del reo ai sensi della normativa italiana anche per fattispecie di reato commesse all'estero. Tra queste, sono compresi anche reati presupposto che assumono rilevanza ai sensi del Decreto, come i reati di abuso di mercato (cfr. Sezione 6 della Parte Speciale).

Inoltre, è importante considerare che la normativa penale dispone, in via generale, la punibilità non soltanto dei soggetti che abbiano materialmente compiuto una determinata fattispecie criminale, bensì anche di qualsiasi soggetto che dia un contributo, materiale o morale, che si ponga in rapporto di causalità, sia pure in termini minimi, nella facilitazione della condotta delittuosa (il c.d., concorso nel reato, artt. 110 e 117 c.p.).

Tenuto conto dei principi sopra indicati, la Banca potrebbe rispondere ai sensi del Decreto anche in connessione con un reato presupposto per il quale un esponente aziendale o dipendente della Banca sia imputabile a titolo di concorso. Inoltre, tale imputabilità a titolo di concorso può realizzarsi anche mediante una condotta (commissiva od omissiva) tenutasi in Svizzera, che sia in concorso con un fatto di reato compiuto in Italia.

I riferimenti normativi contenuti nel presente Modello rinviano alla normativa italiana, ove non diversamente previsto.

2.4. I Destinatari del Modello

Le regole contenute nel Modello 231 si applicano ai seguenti soggetti (i "**Destinatari**") che svolgono attività nell'ambito delle attività sensibili:

- alle persone che rivestono funzioni di rappresentanza, amministrazione, direzione e controllo della Banca ("**Soggetti Apicali**");
- a tutti i dipendenti e a qualsiasi altra persona che presti attività lavorativa, autonoma o subordinata, anche a tempo determinato e/o parziale, a favore della Banca (i "**Collaboratori**").

Al fine di garantire l'efficace ed effettiva prevenzione degli Illeciti Rilevanti, per mezzo di specifiche clausole contrattuali, la Banca richiede anche a soggetti esterni all'organizzazione aziendale che operano quali fornitori di servizi alla Banca stessa (quali, a titolo esemplificativo e non esaustivo i segnalatori di pregi, di seguito "**Procacciatori d'Affari**", e gli External Asset Managers, di seguito "**EAM**") di conoscere il Modello e di rispettarne i principi e le previsioni nell'ambito della relazione contrattuale in essere tra gli stessi e la Banca.

Il Modello ed i contenuti dello stesso sono comunicati ai Destinatari e ai soggetti esterni con modalità idonee ad assicurarne l'effettiva conoscenza, secondo quanto indicato alla successiva Sezione 2.12 della Parte Generale del presente Modello.

Tutti i Destinatari sono tenuti a rispettarne puntualmente tutte le disposizioni del Modello ai medesimi applicabili, anche in adempimento dei doveri di correttezza e diligenza derivanti dal rapporto giuridico da essi instaurato con la Banca.

La Banca condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del presente Modello, anche qualora il comportamento sia realizzato nell'interesse o vantaggio della Banca ovvero con l'intenzione di arrecare ad essa un vantaggio.

2.5. Finalità del Modello

La Banca dispone già di un articolato sistema di controllo interno formalizzato nel proprio corpus normativo. Tuttavia, per attuare il D.Lgs. 231/2001, tali strumenti sono stati integrati con il Modello. La Banca intende così definire un sistema integrato e formalizzato di procedure, controlli e altre misure organizzative al fine di prevenire la commissione degli Illeciti Rilevanti. In particolare, con il presente Modello la Banca intende:

- informare adeguatamente i Destinatari in merito alle attività che comportano il rischio di commissione degli Illeciti Rilevanti e alle conseguenze sanzionatorie che possono derivare ad essi o alla Banca stessa, per effetto della violazione di norme di legge o di disposizioni interne;
- diffondere e affermare una cultura d'impresa improntata alla legalità, con l'espressa riprovazione da parte della Banca di ogni comportamento contrario alla legge o alle disposizioni interne e, in particolare, alle disposizioni contenute nel presente Modello;
- prevedere un'efficiente ed equilibrata organizzazione dell'attività d'impresa, con particolare riguardo alla formazione delle decisioni e alla loro trasparenza, ai controlli, preventivi e successivi, nonché all'informazione interna ed esterna.

Il presente Modello ha natura di normativa interna vincolante per tutti i Destinatari dello stesso e costituisce, pertanto, una componente del generale sistema di organizzazione e controllo interno adottato dalla Banca specificamente finalizzato a garantire lo svolgimento delle attività aziendali nel pieno rispetto della legalità.

2.6. Struttura del Modello

Il presente Modello 231 è strutturato in:

- una Parte Generale, che contiene l'insieme delle regole e dei principi generali dettati dal Modello al fine di delineare un sistema organizzativo e di controllo interno per prevenire la commissione delle fattispecie degli Illeciti Rilevanti, inclusa l'istituzione e il funzionamento dell'Organismo di Vigilanza;
- una Parte Speciale, che indica i principi di comportamento e procedurali finalizzati a prevenire le specifiche tipologie di Illeciti Rilevanti, ciascuno dei quali organizzato con una breve descrizione delle fattispecie di Illeciti Rilevanti, l'individuazione delle attività sensibili e dei principi generali di comportamento e organizzativi.

2.7. Sistema normativo della Banca

Il contesto organizzativo della Banca è costituito dall'insieme di regole, strutture e procedure che garantiscono il funzionamento della Banca (cfr. Norma Operativa 1.2 Apparato Normativo di PKB Private Bank SA).

L'apparato normativo della Banca prevede le seguenti tipologie di documenti (in ordine gerarchico decrescente):

a). Statuto della Banca

Lo Statuto è l'atto fondativo della Banca, nel quale vengono descritte le regole di base di funzionamento e il ruolo degli Organi sociali.

b). Regolamento di Amministrazione e Gestione ("RAG")

Il RAG definisce la struttura organizzativa e le regole amministrative e gestionali applicabili alla Banca e al Gruppo. Il RAG è approvato dal Consiglio di Amministrazione di PKB ed è soggetto all'autorizzazione dell'Autorità federale di vigilanza dei mercati finanziari.

c). Politiche e Regolamenti

Le Politiche (o "Policies") definiscono i principi generali stabiliti dal Consiglio di Amministrazione della Banca per la gestione di specifici rischi o attività. Le stesse danno inoltre indicazione in merito agli strumenti a disposizione per la gestione dei rischi e delle attività, stabiliscono ruoli e responsabilità all'interno della struttura organizzativa di Gruppo.

I Regolamenti determinano le modalità e le misure atte a garantire lo svolgimento di alcune attività di rilievo del Gruppo, in accordo con eventuali politiche di riferimento, e definiscono le linee guida che devono essere osservate dai collaboratori.

d). Norme Operative

Le Norme Operative sono direttive interne approvate dalla Direzione Generale della Banca, che, coerentemente con le Politiche e/o Regolamenti di riferimento, disciplinano i principali processi operativi allo scopo di assicurare il rispetto delle normative legali e delle "acceptable practices" di settore.

e). Processi, Formulari, Istruzioni Operative e Manuali Utente

I Processi rappresentano in modo sintetico input, output e responsabilità relative ad attività della Banca.

Con il termine Formulari si intende la documentazione della Banca destinata ad inquadrare il rapporto con i clienti e la modulistica che viene utilizzata da collaboratori e altre controparti al fine di raccogliere le necessarie autorizzazioni a supporto e completamento di quanto stabilito dalle Norme Operative e dai processi.

Le Istruzioni Operative descrivono lo svolgimento delle attività con l'ausilio degli strumenti specifici che le funzioni operative della Banca hanno adottato.

I Manuali Utente guidano un definito target di collaboratori nell'utilizzo degli strumenti a supporto dell'operatività e sono solitamente legati a una Norma Operativa di cui specificano gli ambiti applicativi.

Tutti i documenti che costituiscono la normativa aziendale ed ogni aggiornamento degli stessi sono pubblicati sull'Intranet della Banca dall'Organizzazione Aziendale, accessibili da parte di tutti i Collaboratori.

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 Destinatari sono tenuti a rispettare, in relazione al tipo di rapporto in essere con la Banca.

2.7.1. La Carta dei Valori di Gruppo

Il Gruppo ha adottato una propria Carta dei Valori di Gruppo, che definisce la sintesi dei valori fondativi del Gruppo, ossia:

- etica professionale;
- integrità morale;
- attenzione ai valori umani e all'equità;
- ricerca dell'eccellenza;
- orientamento al cliente;
- spirito di squadra e collaborazione;
- apertura al cambiamento;
- coerenza;
- responsabilità nell'uso delle risorse.

Si sottolinea come siano previsti quali primi due valori fondamentali:

- il rispetto dell'etica professionale, che include la corretta gestione di conflitti d'interesse e il rispetto da parte di tutti i Collaboratori in ogni circostanza, indistintamente dalla posizione gerarchica e dalle mansioni svolte, di un comportamento deontologicamente ineccepibile, rivolto alla trasparenza ed alla correttezza e atto a tutelare i clienti e la reputazione della Banca; e
- l'integrità morale, che include il pieno rispetto delle norme vigenti e dei principi comportamentali.

La Carta dei Valori contiene anche la sintesi della *vision* del Gruppo.

Tutti i Destinatari ricevono copia della Carta dei Valori di Gruppo al momento dell'assunzione ovvero dell'assunzione del proprio incarico nella Banca. Ogni condotta non conforme alla Carta dei Valori costituisce illecito disciplinare e può comportare la risoluzione del rapporto di impiego

2.7.2. Il Sistema dei Controlli Interni

In conformità con la normativa applicabile, il Gruppo ha adottato un proprio Sistema di Controllo Interno ("**SCI**"), quale insieme delle strutture e dei processi di controllo che a tutti i livelli organizzativi delle singole entità del Gruppo supportano il raggiungimento degli obiettivi di politica commerciale e il corretto funzionamento del Gruppo e della singola entità (cfr. Regolamento sul Sistema di Controllo Interno del Gruppo PKB; Norma Operativa Sistema di Controllo Interno (SCI)).

Lo SCI del Gruppo si prefigge di:

- sostenere la realizzazione degli obiettivi strategici del Gruppo;
- permettere di sorvegliare il rispetto delle leggi e dei regolamenti vigenti in ciascun Paese in cui le singole entità del gruppo hanno sede e/o operano;
- proteggere il patrimonio del Gruppo;
- contribuire alla mitigazione dei vari rischi presenti nell'attività del Gruppo;
- scoprire, limitare ed evitare gli eventuali errori e altre irregolarità che possono generarsi nello svolgimento delle attività;
- garantire l'affidabilità e la completezza della struttura contabile e la pubblicazione di rapporti attendibili e puntuali, incluso l'integralità delle chiusure finanziarie e l'allestimento dei rendiconti economici;

- fornire le informazioni necessarie a dirigere efficacemente il Gruppo e le singole entità che lo compongono.

Il SCI si basa sui seguenti principi di architettura:

- principio dei "quattro occhi", che viene perseguito attraverso la suddivisione delle attività/responsabilità, relative a un determinato processo, tra differenti funzioni ("*segregation of duties*"), lo svolgimento di verifiche incrociate e di duplici controlli;
- identificazione delle responsabilità delle informazioni e dei processi ("*accountability*"), con l'obiettivo di definire le responsabilità nei confronti degli organi superiori;
- tracciabilità (e non ripudiabilità) dei dati e delle informazioni, con l'obiettivo di rendere attendibile, ricostruibile e valutabile un'attività o un processo;
- identificazione continua delle anomalie (elementi e processi non conformi) e delle relative misure correttive, con l'obiettivo di consentire la mitigazione di errori e anomalie al fine di migliorare i processi.

Il SCI si articola su tre livelli:

a). Prima linea di difesa - responsabile dei rischi generati dalle attività di business

Nella prima linea di difesa si collocano i responsabili delle unità di fronte orientate a generare utili, e/o che, tramite lo svolgimento delle loro attività, generano dei rischi operativi per la Banca.

In questo ambito si collocano primariamente le Divisioni Private e Corporate Banking, le aree Asset Management e Capital Markets, nonché la Divisione Operations, Organisations & ICT ed il Credit Office quali centri di supporto, in relazione alle loro attività operative di primo livello. A tali funzioni spetta la responsabilità per la definizione del sistema di controllo di primo livello.

I responsabili di tali funzioni svolgono la loro funzione di controllo nel quadro delle attività quotidiane tramite la gestione del rischio, in particolare mediante monitoraggio, gestione e reportistica. I relativi controlli di primo livello possono essere insiti nei processi operativi o programmati come attività pianificate a complemento dei processi stessi.

b). Seconda linea di difesa - supervisione indipendente del rischio

Nella seconda linea di difesa sono posizionate le istanze di controllo indipendenti, poste gerarchicamente sotto la responsabilità del CRO, ed in particolare:

- Risk Management;
- Legal & Compliance; e
- il Credit Office (CO) in relazione alle sue attività di supervisione indipendente di secondo livello del rischio di credito.

Le istanze di controllo indipendenti assicurano l'adeguatezza del Sistema di Controllo Interno, supportano il CRO nell'assicurare un adeguato approccio da parte del Gruppo alla cultura del controllo dei rischi e, coerentemente con le aree di responsabilità a loro attribuite e tramite la redazione e implementazione di specifiche Norme Operative, definiscono i limiti operativi entro i quali le unità di primo livello sono autorizzate ad operare coerentemente al sistema di soglie di rischio definito nel *Risk Appetite Framework* del Gruppo; inoltre supervisionano la gestione dei rischi ed il rispetto delle prescrizioni legali, normative interne in relazione alle attività svolte dalla prima linea tramite controlli della coerenza dell'operatività con le soglie di rischio definite

dagli organi aziendali competenti. Infine, le funzioni di controllo indipendenti supportano il CRO nell'assicurare la formazione del personale in materia di gestione del rischio.

In aggiunta rientrano nella seconda linea di difesa le attività di verifica indipendenti svolte dalle Risorse Umane, Contabilità e Bilancio, Pianificazione Strategica e dalla Divisione Operations, Organisations & ICT (con specifico riferimento al Gruppo ICT e all'ufficio Logistica/Sicurezza) nell'esecuzione dei compiti e responsabilità a loro attribuiti.

c). Terza linea di difesa - assurance indipendente

La Terza linea di difesa si focalizza sulla Revisione Interna, la quale svolge verifiche e valutazioni indipendenti ed obiettive sull'adeguatezza ed efficacia dell'organizzazione aziendale e dei processi operativi, delle attività di controllo e supervisione in capo alla prima e alla seconda linea di difesa.

I compiti e le responsabilità della Revisione Interna sono descritti nel "Regolamento sulla Revisione Interna".

In generale, il Gruppo prevede che, per tutte le persone impiegate e in qualsiasi grado gerarchico, sia diffusa un'appropriata cultura del rischio che si rispecchi anche nel sistema di remunerazione.

Si precisa che con riferimento, in generale, ai rischi (di risarcimento a terzi e/o di sanzioni amministrative e/o penali) connessi alla violazione delle norme di legge, legali e di autoregolamentazione che regolano l'attività della Banca e delle sue società controllate, non vi è alcuna propensione al rischio di non conformità alle norme. Non è cioè ammesso alcun tipo di violazione consapevole di tali norme da parte della Banca e dalle sue società controllate. Inoltre, il Gruppo instaura relazioni con clientela che rispetta la normativa fiscale applicabile ("Tax compliance") e limita le relazioni con clientela che potrebbero comportare un rischio accresciuto (ad esempio soggetti domiciliati in giurisdizioni non trasparenti o PEP); la nuova clientela è sottoposta a un processo di accettazione che comporta una valutazione dettagliata preventiva e una rivalutazione periodica della clientela esistente (cfr. Sezione 7 e Sezione 8 della Parte Speciale del presente Modello).

Con particolare riferimento ai reati di antiriciclaggio, sono state adottate specifiche policy e norme operative che disciplinano i processi interni di adeguata verifica della clientela - in fase sia di c.d. *onboarding*, sia in corso di rapporto contrattuale -, di monitoraggio continuo dell'operatività della clientela e di segnalazione delle operazioni sospette alle autorità competenti. I presidi e i controlli previsti da tali policy e Norme Operative sono riassunti nella Sezione della Parte Speciale relativa ai "*Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e autoriciclaggio (art. 25-octies) e reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater)*" (Cfr. Sezione 7 della Parte Speciale del presente Modello).

2.7.3. Il sistema dei poteri e delle deleghe

La Banca è dotata di strumenti organizzativi improntati a principi generali di:

- conoscibilità all'interno della Banca a tutti i livelli aziendali;
- chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna Funzione nonché dei relativi poteri;
- chiara descrizione delle linee di riporto e separazione dei ruoli.

Il Regolamento di Amministrazione e Gestione definisce la struttura organizzativa e le regole amministrative e gestionali applicabili alla Banca e al Gruppo e riporta in allegato il Macro-Organigramma Funzionale del Gruppo. La struttura organizzativa della Banca comprende:

- il Consiglio di Amministrazione e i Comitati del Consiglio di Amministrazione;
- la Direzione Generale ("**DG**");
- il Group Management Committee ("**GMC**");
- i Comitati della DG e di Gruppo.

La Banca, poi, è suddivisa in divisioni operative - ciascuna operante sotto la responsabilità di un membro della DG - alle quali sono conferiti compiti di gestione diretta delle operazioni riferite ai diversi affari e attività della Banca (le "**Divisioni**"), ed in particolare:

- Divisione Private Banking;
- Divisione Domestic & Corporate Banking;
- Divisione Operations, Organisation & ICT;
- Divisione Risk Management, Compliance, Controlli e Credit Office;
- Divisione Finance & Markets.

La Divisioni Private Banking e Domestic & Corporate Banking si compongono di team di consulenti e di un desk dedicato alla gestione delle relazioni con gli intermediari finanziari. All'interno delle Divisioni sono stati definiti dei responsabili per alcune aree di mercato di riferimento. Le altre Divisioni sono invece organizzate in gruppi identificati in base alla tipologia di attività svolta.

All'interno della Banca esistono poi unità operative e/o di staff che dipendono da un membro della DG, ed in particolare:

- Asset Management;
- Risorse Umane;
- Segreteria Generale.

Le mansioni e le competenze di tutti i collaboratori della Banca sono stabilite individualmente in funzione dell'attività svolta e descritte nello specifico mansionario individualmente attribuito il quale stabilisce anche il superiore gerarchico di riferimento a cui il Collaboratore risponde per il proprio operato ([1]).

([1]) L'ordinamento gerarchico della Banca prevede i seguenti gradi:
- Direttore generale;
- Condirettore generale;
- Direttore;
- Condirettore;
- Vicedirettore;
- Procuratore capo;
- Procuratore;
- Mandatario commerciale;
- Impiegato.

Le regole generali che disciplinano il rapporto di lavoro tra la Banca ed il personale sono contenute nel "*Regolamento per il personale*" e, ove non contemplate dal predetto regolamento, nelle disposizioni legali svizzere applicabili ai contratti di lavoro.

Viene conferito potere di firma a tutti i Collaboratori con almeno grado di mandatario commerciale. Per impegnare giuridicamente la Banca è necessaria la firma collettiva di due persone autorizzate a firmare in suo nome come indicato nel Registro delle imprese del Canton Ticino ([2]).

2.8. Organismo di Vigilanza

2.8.1. Nomina dell'Organismo di Vigilanza

Il Decreto richiede, quale condizione necessaria per escludere la responsabilità amministrativa, che il compito di vigilare sul funzionamento e sull'osservanza del Modello sia affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo, senza disporre di poteri gestionali e/o amministrativi.

A tal fine, il Consiglio di Amministrazione della Banca nomina, su proposta dell'Audit & Risk Commitee ("**ARC**") e previo accordo da parte del Comitato Nomine e Remunerazioni ("**CNR**"), un organismo di vigilanza (l'"**Organismo di Vigilanza**" o "**ODV**") quale organo collegiale composto da membri interni e membri esterni, secondo la composizione che sarà di volta in volta stabilita dal Consiglio di Amministrazione secondo le necessità.

In sede di nomina, il Consiglio di Amministrazione stabilisce anche il compenso annuale dei membri esterni dell'ODV, in misura fissa per l'intero mandato, su proposta del CNR. Il compenso stabilito nella delibera di nomina può essere adeguato in caso di ampliamento del catalogo dei reati, di cambiamenti nell'assetto organizzativo dell'ente o di una estensione delle attività svolte in conseguenza alle variazioni di rischio.

L'ODV propone annualmente all'ARC una proposta di dotazione finanziaria per lo svolgimento delle proprie attività, che viene discussa e concordata tra l'ODV e l'ARC stesso prima della presentazione al Consiglio di Amministrazione. Il Consiglio di Amministrazione, su proposta dell'ODV, concordata con l'ARC e formalizzata da parte di quest'ultimo, assegna annualmente all'Organismo di Vigilanza una dotazione adeguata di risorse finanziarie, che il medesimo potrà utilizzare per ogni esigenza necessaria al corretto svolgimento dei propri compiti.

2.8.2. Requisiti di eleggibilità dei membri dell'ODV

I membri dell'Organismo di Vigilanza devono essere in possesso dei requisiti di onorabilità, professionalità e indipendenza che vengono specificati qui di seguito.

Il possesso di tali requisiti in capo ai membri dell'Organismo di Vigilanza viene previamente accertato dall'ARC, che informa il Consiglio di Amministrazione ai fini della relativa nomina e, in seguito ogni anno, dall'Organismo di Vigilanza stesso.

La mancanza o la perdita dei seguenti requisiti di onorabilità, professionalità e indipendenza comporta

([2]) I mandatari commerciali possono firmare solo congiuntamente con un membro di direzione o con un procuratore. I poteri conferiti ai mandatari commerciali ai sensi dell'art. 462 del Codice delle Obbligazioni svizzero si estendono anche al diritto di firmare e girare assegni, ma non di emettere, accettare, girare e avallare cambiali. I membri della Revisione interna firmano singolarmente e solo nell'espletamento delle loro incombenze, ossia unicamente nei casi e per i compiti strettamente legati e conseguenti alle loro funzioni ispettive, con esclusione di firma per tutto quanto concerne il normale svolgimento dei processi operativi.
Il Consiglio di Amministrazione è autorizzato a concedere, in casi particolari, il diritto di firma individuale, in deroga alla firma collettiva.

la decadenza dalla carica di membro dell'Organismo di Vigilanza.

- *Requisiti di onorabilità*

I membri dell'Organismo di Vigilanza devono possedere i seguenti requisiti di onorabilità:

a). non si trovano in una delle condizioni di ineleggibilità o decadenza previste dall'articolo 2382 del codice civile ([3]);
b). non sono stati condannati a seguito di sentenza, ancorché non ancora definitiva o emessa ex artt. 444 e ss. c.p.p. o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
   i. alla reclusione per un tempo non inferiore ad un anno per uno dei delitti previsti dal regio decreto 16 marzo 1942 n. 267 (Legge Fallimentare);
   ii. a pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia e valori mobiliari, di strumenti di pagamento;
   iii. alla reclusione per un tempo non inferiore ad un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;
   iv. per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore a due anni;
   v. per uno dei reati societari previsti dal titolo XI del libro V del codice civile, espressamente richiamati dal Decreto;
   vi. per un reato che importi ed abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
   vii. per uno o più illeciti tra quelli tassativamente previsti dal Decreto.
c). non hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società o altri enti nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto;
d). non sono stati sottoposti all'applicazione, in via definitiva, ad una delle misure di prevenzione previste dal D.Lgs. 6 settembre 2011, n. 159 "Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia";
e). non sono stati sottoposti all'applicazione delle sanzioni amministrative accessorie previste dall'art. 187 *quater* del D.Lgs. 58/1998 ("TUF");
f). non sono stati destinatari di provvedimenti iscritti nel casellario giudiziale e nel casellario dei carichi pendenti;
g). non sono stati sottoposti a procedimenti penali nonché di patteggiamento ad una pena che comporti interdizione anche temporanea dai pubblici uffici.

- *Requisiti di professionalità*

Al fine di dotare l'Organismo di Vigilanza di competenze professionali adeguate al migliore svolgimento delle funzioni ad esso assegnate, almeno uno dei membri effettivi deve essere scelto tra esperti (quali, ad esempio, docenti o liberi professionisti) in materie giuridiche, economiche, finanziarie o tecnico-scientifiche o comunque tra soggetti in possesso di competenze specialistiche adeguate alla funzione derivanti, ad esempio, dall'aver svolto per un congruo periodo di tempo attività

([3]) Ossia, non devono essere soggetti interdetti, inabilitati, falliti, coloro che sono stati condannati ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi

professionali in materie attinenti al settore nel quale la Banca opera e/o dall'avere una adeguata conoscenza dell'organizzazione, dei sistemi dei controlli e dei principali processi aziendali ovvero dell'aver fatto – o di fare – parte di Organismi di Vigilanza di altri istituti operanti nell'ambito bancario, finanziario o assicurativo.

- *Requisiti di indipendenza*

Al fine di garantire l'autonomia e l'indipendenza, i membri esterni dell'Organismo di Vigilanza non devono:

- aver rapporti d'affari, né trovarsi in una posizione - neppure potenziale - di conflitto d'interessi con la Banca;
- avere legami di parentela, affinità (entro il quarto grado) o convivenza con i soggetti Destinatari.

Inoltre, al fine di garantire l'indipendenza dei membri dell'Organismo di Vigilanza è opportuno che i medesimi interni non siano titolari all'interno della Banca di funzioni di tipo operativo o di *business*, che ne minerebbero l'obiettività di giudizio nel momento delle verifiche sul rispetto del Modello.

2.8.3. Durata in carica, decadenza e revoca dei membri dell'ODV

- *Durata*

L'Organismo di Vigilanza rimane in carica per tre anni, con possibilità di rinnovo per ulteriori periodi della stessa durata da parte del Consiglio di Amministrazione.

La validità della nomina dei membri dell'Organismo di Vigilanza è subordinata al preventivo accertamento dei requisiti di onorabilità, professionalità e indipendenza indicati sopra, che costituiscono un requisito essenziale per rimanere in carica. Tale accertamento può essere effettuato attraverso l'analisi del curriculum vitae e il rilascio di specifiche autodichiarazioni da parte dei candidati.

Alla scadenza dell'incarico, l'Organismo di Vigilanza continua a svolgere le proprie funzioni e ad esercitare i propri poteri fino alla nomina dei nuovi componenti.

- *Decadenza e revoca*

I componenti dell'Organismo di Vigilanza cessano dalla relativa carica, oltre che nel caso di scadenza del mandato conferito, qualora si verifichino una o più cause di decadenza e/o revoca qui di seguito specificate.

Costituiscono cause di decadenza dei componenti dell'Organismo di Vigilanza:

- il venir meno dei requisiti di onorabilità e indipendenza;
- la sopravvenuta morte o incapacità giuridica;
- le dimissioni volontarie dalla carica di membro dell'Organismo di Vigilanza;
- eventuali dimissioni o licenziamento dei membri interni alla struttura aziendale.

La decadenza ha effetto di diritto, dal momento in cui si verifica la relativa causa.

I componenti dell'Organismo di Vigilanza non possono essere revocati, se non per giusta causa. La revoca dei membri dell'Organismo di Vigilanza è di competenza del Consiglio di Amministrazione. Costituisce, a titolo esemplificativo, giusta causa di revoca:

- una sentenza di condanna della Banca o di patteggiamento per la commissione degli Illeciti Rilevanti, passata in giudicato e dalla quale si evince che la vigilanza sul Modello da parte dell'Organismo di Vigilanza stesso è stata omessa o insufficiente e/o un difetto di onorabilità e indipendenza dei suoi membri;
- la violazione degli obblighi di riservatezza;
- l'assenza ingiustificata a più di due riunioni consecutive dell'Organismo di Vigilanza;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "*autonomia e indipendenza*" e "*continuità di azione*" propri dell'OdV;
- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico (a titolo esemplificativo e non esaustivo, mancato adempimento di più della metà delle attività previste nel Piano annuale, salvo cause di forza maggiore, il mancato avvio di controlli interni a seguito di segnalazioni di violazioni del Modello o di condotte illecite).

Le cause di decadenza e di revoca sono comunicate all'Organismo di Vigilanza dai diretti interessati o da chiunque ne venga a conoscenza. L'Organismo di Vigilanza può anche rilevare autonomamente, nell'esercizio delle proprie attività, eventuali cause di decadenza o revoca dei propri membri.

L'Organismo di Vigilanza comunica, senza indugio, ogni causa di decadenza o di revoca all'ARC e al Consiglio di Amministrazione. In caso di segnalazione di cause di revoca, il Consiglio di Amministrazione, previa analisi dei fatti e delle relative prove da parte dell'ARC, delibera in merito alla revoca o decadenza dei membri dell'ODV interessati, motivando nel verbale la propria decisione.

In caso di revoca o decadenza di uno dei membri dell'Organismo di Vigilanza, il Consiglio di Amministrazione, su proposta dell'ARC e previo accordo da parte del CNR, provvede alla nomina di un nuovo componente. Il componente nominato in sostituzione del componente revocato o decaduto rimane in carica fino alla scadenza del mandato conferito all'intero Organismo di Vigilanza.

L'intero Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso il Consiglio di Amministrazione deve nominare un nuovo Organismo di Vigilanza.

2.8.4. Funzioni e poteri dell'Organismo di Vigilanza

I membri dell'Organismo di Vigilanza devono adempiere ai loro doveri con la diligenza del mandatario e sono responsabili della verità delle loro attestazioni.

La collegialità dell'Organismo di Vigilanza non esclude una ripartizione interna dei compiti, fermo restando che gli esiti delle attività di vigilanza espletate individualmente tramite le linee di difesa della Banca od eventuali esterni, devono formare oggetto di riesame collegiale.

L'Organismo di Vigilanza nello svolgimento delle proprie funzioni opera sulla base di uno specifico regolamento approvato dal medesimo. In particolare, l'Organismo di Vigilanza esegue i compiti di propria competenza nel rispetto delle politiche aziendali interne, evitando di ostacolare le ordinarie attività lavorative della Banca.

L'Organismo di Vigilanza è completamente autonomo nell'esplicazione dei suoi compiti. Al fine di garantire l'efficacia dell'attività svolta dall'Organismo di Vigilanza e l'impossibilità che tale attività possa ingenerare forme di ritorsione a danno del detto organismo o dei soggetti ai quali quest'ultimo abbia richiesto collaborazione o supporto, tutte le attività e le determinazioni dell'Organismo di Vigilanza non possono essere sindacate da alcun organismo o struttura aziendale.

Ogni informazione, segnalazione, comunicazione, report, previsti nel presente Modello, nonché tutta la documentazione prodotta nell'esercizio delle relative funzioni è conservata dall'Organismo di Vigilanza in un apposito archivio riservato (informatico e/o cartaceo) per un periodo di 10 anni, e comunque nel rispetto di quanto previsto dalla normativa applicabile in materia di trattamento dei dati personali.

L'accesso all'archivio è consentito esclusivamente all'Organismo di Vigilanza, all'ARC e al Consiglio di Amministrazione.

2.8.5. Periodicità delle riunioni, validità delle deliberazioni e verbalizzazione

L'Organismo di Vigilanza si riunisce con periodicità almeno trimestrale e ogniqualvolta sia ritenuto necessario e/o opportuno dal Presidente o da altro membro, ed in particolare in occasione di modifiche rilevanti nella normativa di riferimento e/o nella struttura organizzativa della Banca o del Gruppo.

La riunione è convocata dal Presidente presso la sede sociale della Banca o altrove, purchè in Svizzera.

L'Organismo di Vigilanza può riunirsi anche con collegamento dei partecipanti in video-teleconferenza o mediante collegamento telefonico.

Per la validità delle deliberazioni è necessario il voto favorevole della maggioranza dei membri dell'ODV in carica.

2.8.6. I compiti e poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono affidati i seguenti compiti e poteri:

- vigilare sul funzionamento e l'osservanza del Modello;
- verificare l'effettiva idoneità del Modello a prevenire la commissione degli Illeciti Rilevanti;
- analizzare la persistenza nel tempo dei requisiti di solidità e funzionalità del Modello;
- curare, sviluppare e promuovere il costante aggiornamento del Modello, suggerendo, ove necessario, al Consiglio di Amministrazione della Banca le correzioni e gli adeguamenti dovuti;
- mantenere i rapporti e assicurare i flussi informativi di competenza verso l'organo amministrativo della Banca;
- acquisire informazioni e documentazione di ogni tipo da ogni livello e settore della Banca per le attività rilevanti ai sensi del Modello;
- compiere verifiche ed ispezioni al fine di accertare eventuali violazioni del Modello;
- elaborare un piano delle attività previste, in coerenza con i principi contenuti nel Modello;
- assicurare l'attuazione del piano di attività previste;
- assicurare l'elaborazione della reportistica sulle risultanze degli interventi effettuati;
- assicurare il costante aggiornamento del sistema di identificazione, mappatura e classificazione delle aree di rischio ai fini dell'attività di vigilanza propria dell'Organismo di Vigilanza;
- definire e promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché della formazione del personale e della sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
- fornire chiarimenti in merito al significato e all'applicazione delle previsioni contenute nel Modello;
- curare l'efficacia del sistema di segnalazione (c.d. whistleblowing) instituito ai sensi del Modello e la sua conformità ai requisiti previsti dal Decreto;

- formulare la previsione di spesa per lo svolgimento della propria attività da sottoporre alla preventiva analisi e discussione con l'ARC e successivamente all'approvazione del Consiglio di Amministrazione della Banca; eventuali spese straordinarie dovranno essere parimenti sottoposte alla preventiva analisi e discussione con l'ARC e all'approvazione dello stesso Consiglio di Amministrazione della Banca;
- promuovere l'attivazione di eventuali procedimenti disciplinari e/o sanzioni presso i competenti organi e funzioni della Banca riferiti a violazioni del Modello (per una descrizione delle possibili violazioni del Modello cfr. Sezione 2.10 della Parte Generale del presente Modello).

All'Organismo di Vigilanza sono conferiti i più ampi e autonomi poteri di iniziativa e controllo al fine di vigilare in modo adeguato ed efficiente sul funzionamento e l'osservanza del Modello, ed in particolare a titolo esemplificativo i seguenti poteri (da esercitarsi nell'ambito dei compiti propri dell'ODV):

- accedere a tutti i documenti e a tutte le informazioni relative alla Banca;
- avvalersi di tutte le strutture della Banca, che sono obbligate a collaborare, dei revisori e dei consulenti esterni;
- raccogliere informazioni e chiedere l'esibizione di documenti o l'estrazione di dati aziendali a tutti i Collaboratori in relazione alle attività della Banca;
- richiedere, attraverso i canali e le persone appropriate, la riunione del Consiglio di Amministrazione per affrontare questioni urgenti;
- richiedere ai Responsabili di Funzione di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza.

L'Organismo di Vigilanza non ha poteri coercitivi o di intervento sulla struttura aziendale o sanzionatori, poteri questi che sono demandati alle funzioni aziendali competenti.

2.8.7. Obbligo di collaborazione e supporto all'Organismo di Vigilanza

Nello svolgimento dei propri compiti di vigilanza e di controllo l'Organismo di Vigilanza è costantemente supportato dai Responsabili di Funzione e, in generale, da tutti i Collaboratori.

In particolare, i Responsabili di Funzione sono tenuti a:

- controllare le attività e le aree di propria competenza;
- verificare l'osservanza del Modello da parte dei Collaboratori sottoposti alla loro direzione;
- segnalare tempestivamente e puntualmente all'Organismo di Vigilanza le informazioni relative ad eventuali anomalie, problematiche e/o criticità rilevate.

L'Organismo di Vigilanza potrà richiedere alla Revisione Interna, sentito l'ARC, specifiche attività di controllo sul corretto e preciso funzionamento del Modello.

Tutti i soggetti coinvolti all'interno della struttura aziendale sono tenuti ad informare l'Organismo di Vigilanza sulla mancata applicazione del presente Modello, ciascuno nell'ambito delle proprie competenze operative.

2.9. Flussi informativi da e verso l'Organismo di Vigilanza

2.9.1. Flussi informativi dall'Organismo di Vigilanza ai vertici aziendali

L'Organismo di Vigilanza trasmette, con periodicità annuale, all'ARC e al Consiglio di Amministrazione una relazione contenente:

- le attività e i controlli svolti in corso d'anno, specificando le eventuali criticità e le eventuali violazioni del Modello eventualmente riscontrate nonché una proposta di piano di implementazione di misure correttive necessarie;
- le eventuali proposte di aggiornamento e/o revisione del Modello;
- il piano delle attività che intende svolgere nell'anno successivo per adempiere ai compiti assegnatigli.

L'Organismo di Vigilanza segnala immediatamente all'ARC e al Consiglio di Amministrazione eventuali problematiche significative emerse dalle attività che meritano interventi immediati (come ad es. la commissione di gravi violazioni del Modello).

Il Consiglio di Amministrazione ha la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza.

L'Organismo di Vigilanza potrà, inoltre, organizzare incontri con i Soggetti Apicali e i Collaboratori addetti allo svolgimento di attività sensibili al fine di analizzare congiuntamente eventuali rischi di commissione degli Illeciti Rilevanti nell'ambito delle stesse o recepire qualsiasi altra informazione possa essere utile all'adempimento dei propri compiti.

2.9.2. Flussi informativi dalle Funzioni aziendali all'Organismo di Vigilanza

All'ODV devono essere comunicate, a cura dell'ARC o del Presidente del Consiglio di Amministrazione, notizie occasionali, relative alla gestione societaria e ad eventi, rispetto ai quali è opportuna un'informativa tempestiva nei confronti dell'ODV.

A titolo esemplificativo e ove rilevante rispetto agli ambiti di applicazione del Modello:

- i provvedimenti e/o le notizie provenienti dall'autorità giudiziaria competente, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini/accertamenti, riguardanti la Banca, anche nei confronti di ignoti, per i reati o gli illeciti amministrativi di cui al Decreto;
- eventuali anomalie significative riscontrate nell'attività di verifica, svolta dalla funzione interne di controllo;
- le notizie relative alle variazioni organizzative e procedurali significative ai fini del Modello;
- l'articolazione dei poteri e il sistema delle deleghe adottato dalla Banca ed eventuali modifiche che intervengano sullo stesso;
- la documentazione relativa all'attività di informazione e formazione svolta in attuazione del Modello e alla partecipazione alla medesima da parte del personale;
- la documentazione relativa agli esiti delle attività di ispezione, verifica e monitoraggio compiute da parte delle Autorità di vigilanza, con riferimento a ove rilevante per il Modello;
- report prodotti nell'ambito dei piani di controllo periodici previsti dalla Banca.

Fermo quanto sopra, la funzione Compliance assicura un'informativa annuale all'ODV segnalando in ogni caso, tempestivamente, gli eventi che possono compromettere l'efficacia del Modello. La Funzione di Revisione Interna trasmetterà tutti i rapporti di revisione rilevanti per il Modello ad un membro dell'ODV che riferirà nel corso delle sedute agli altri membri i fatti rilevanti.

2.10. Il sistema sanzionatorio

Le disposizioni e le regole di condotta di cui al presente Modello 231 sono obbligatorie per ogni Destinatario e, con specifico riferimento ai Collaboratori, integrano le obbligazioni oggetto del relativo rapporto di lavoro, in aggiunta a quelle previste dalla legge, dalla normativa interna e dai rispettivi contratti di lavoro.

La violazione delle previsioni del Modello potrà determinare, dunque, l'apertura di un procedimento disciplinare nei confronti del Collaboratore e l'eventuale applicazione di provvedimenti disciplinari secondo le modalità previste dalle specifiche previsioni adottate della Banca (cfr. Norma Operativa 4 Personale 4.24 Sanzioni disciplinari).

L'esperimento di un procedimento disciplinare - e l'irrogazione di una sanzione disciplinare - nei confronti del Collaboratore si intende comunque indipendente da eventuali procedimenti penali e/o amministrativi e/o regolamentari, etc. avviati dalle autorità competenti - specie nel caso in cui il comportamento del Collaboratore possa integrare una fattispecie di Illecito Rilevante - e comunque non preclusivo del diritto della Banca di intraprendere ogni ulteriore iniziativa ed azione, anche ai fini di ottenere il risarcimento di danni causati, connessi od anche solo occasionati dalla condotta del Collaboratore.

Costituiscono violazioni del Modello, a titolo esemplificativo:

- comportamenti che integrino, direttamente o indirettamente, un Illecito Rilevante;
- comportamenti che, sebbene non configurino uno degli Illeciti Rilevanti, siano diretti in modo univoco alla loro commissione;
- comportamenti non conformi alle procedure richiamate nel Modello al fine di ridurre il rischio di commissione di uno degli Illeciti Rilevanti ovvero non conformi ai protocolli previsti nel Modello o richiamati dallo stesso;
- un comportamento non collaborativo nei confronti dell'ODV, consistente a titolo esemplificativo e non esaustivo, nel rifiuto di fornire le informazioni o la documentazione richiesta, nel mancato rispetto delle direttive generali e specifiche rivolte dall'ODV al fine di ottenere le informazioni ritenute necessarie per l'assolvimento dei propri compiti, nella mancata partecipazione senza giustificato motivo alle visite ispettive programmate dall'ODV, nella mancata partecipazione agli incontri di formazione;
- violazione degli obblighi di informazione e/o segnalazione verso l'ODV;
- violazioni delle misure di tutela di ogni soggetto che ha effettuato una segnalazione (c.d. *whistleblower*);
- l'effettuazione con dolo o colpa grave di segnalazioni che si rivelano infondate.

Qualsiasi tipo di violazione delle regole comportamentali contenute nel Modello autorizza l'ODV a richiedere al soggetto titolare del potere disciplinare della Banca l'irrogazione di una delle sanzioni di seguito indicate.

Le sanzioni applicabili ai Collaboratori in caso di violazioni del presente Modello - ordinate per gravità secondo quanto previsto dalla relativa normativa interna della Banca (cfr. Norma Operativa 4.24 "*sanzioni disciplinari*") - sono:

a). richiamo verbale;
b). richiamo scritto;
c). ammonimento formale;
d). ammonimento severo accompagnato da comminatoria che in caso di recidiva si procederà alla rescissione del rapporto di lavoro);
e). modifica delle condizioni contrattuali;
f). sospensione dal servizio (con o senza remunerazione);
g). licenziamento nel rispetto del termine di disdetta;
h). licenziamento immediato per causa grave.

Tutte le sanzioni possono avere un impatto sulla remunerazione variabile.

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

- intensità del dolo o della colpa;
- eventuale condotta recidiva;
- entità del pericolo e/o delle conseguenze della violazione per la Banca;
- prevedibilità delle conseguenze della condotta in violazione;
- tempi e i modi della violazione;
- altre circostanze nelle quali la violazione ha avuto luogo.

In caso di violazione del Modello da parte di uno o più componenti del Consiglio di Amministrazione, l'ODV informerà l'intero Consiglio di Amministrazione, che prenderà gli opportuni provvedimenti coerentemente con la gravità della violazione commessa alla luce dei criteri indicati nella PRESENTE Sezione 2.10 e conformemente ai poteri previsti dalla legge e/o dallo statuto della Banca.

Qualora il Consiglio di Amministrazione fosse informato in merito a violazioni del Modello da parte di uno o più membri dell'ODV, il Consiglio di Amministrazione provvederà ad assumere le iniziative ritenute più idonee coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto.

In particolare, qualora la violazione sia commessa da un componente dell'OdV che sia anche un Collaboratore della Banca si applicheranno le sanzioni sopra indicate con riferimento ai Collaboratori.

Le condotte di soggetti esterni alla Banca, che cooperano con la Banca nell'ambito delle attività sensibili, che siano potenzialmente in contrasto o in violazione del presente Modello comporteranno – a seconda dei relativi obblighi contrattuali - nelle ipotesi di minore gravità la richiesta da parte della Banca di sostituire il soggetto che abbia posto in essere il comportamento (ove possibile) e/o, nelle restanti ipotesi, la risoluzione anticipata del rapporto contrattuale.

L'applicazione o meno delle suddette misure non preclude, comunque, il diritto della Banca di intraprendere, ove ne ricorrano i presupposti, ogni iniziativa e azione anche cautelare e/o finalizzata ad ottenere l'inibitoria degli eventuali comportamenti posti in essere dai soggetti esterni in contrasto o in violazione del presente Modello, così come non preclude di agire per ottenere il ristoro di qualsivoglia eventuale danno/pregiudizio verificatosi in conseguenza di condotte non conformi e/o inadempienti alle medesime previsioni.

2.11. Sistemi di segnalazione (*whistleblowing*)

- *Sistema di segnalazione*

Ai sensi dell'art. 6, co. 2-bis, del Decreto il Modello deve prevedere l'istituzione di un canale di comunicazione, che consenta ai Destinatari di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del Modello dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte. La stessa previsione normativa richiede anche di prevedere che:

- tale canale di comunicazione garantisca la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
- vi sia almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

- vi sia un divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- vi siano nel sistema disciplinare adottato sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

In conformità con il Decreto, la Banca ha istituito nell'ambito del Modello degli specifici canali di segnalazioni attraverso i quali i Destinatari sono tenuti ad effettuare segnalazioni con tempestività qualora vengano a conoscenza di condotte illecite ai sensi del Decreto e/o violazioni del presente Modello (tali violazioni sono definite nella Sezione 2.10 del presente Modello).

Il mancato adempimento di tale obbligo di segnalazione costituisce di per sé un illecito disciplinare e/o una violazione contrattuale e potrà determinare l'irrogazione di una sanzione disciplinare, che potrà variare a seconda della gravità dell'inottemperanza.

- *La segnalazione*

Il segnalante deve fornire tutti gli elementi utili a consentire all'Organismo di Vigilanza di procedere alle dovute ed appropriate verifiche ed agli accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione. A tal fine, la segnalazione deve preferibilmente contenere i seguenti elementi:

- generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta;
- una chiara e completa descrizione dei fatti oggetto di segnalazione;
- se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi i fatti;
- se conosciute, le generalità o altri elementi (come la qualifica e il servizio in cui svolge l'attività) che consentano di identificare il soggetto/i che ha/hanno posto in essere i fatti segnalati;
- l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- l'indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

Possono anche essere trasmesse segnalazioni anonime, purchè siano fondate su elementi di fatto precisi e concordanti.

Le segnalazioni possono essere trasmesse via email al seguente indirizzo odv@pkb.ch ovvero via posta, al seguente recapito:

Alla c.a. dell'Organismo di Vigilanza ex D.Ls. 231/2001

PKB Private Bank SA

Via S. Balestra, n. 1

CH 6901 - Lugano

In via alternativa, le segnalazioni possono essere trasmesse al responsabile della Funzione Internal Audit. Il Responsabile della Funzione Internal Audit provvederà a trasmettere la segnalazione all'Organismo di Vigilanza, salvo nell'ipotesi in cui la segnalazione riguardi i membri dell'Organismo di Vigilanza, nel qual caso gli accertamenti sulla segnalazione saranno svolti dallo stesso in conformità con quanto previsto nella presente Sezione.

In ogni caso, la Banca garantisce i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione ed assicura la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge e la tutela dei diritti della Banca stessa o delle persone accusate erroneamente e/o in mala fede.

La tutela del segnalante sarà supportata anche da un'efficace attività di sensibilizzazione e comunicazione per i Collaboratori nell'ambito della formazione prevista sul Modello (cfr. Sezione 2.12). I Destinatari saranno informati in merito alla possibilità di effettuare segnalazioni all'ODV tramite apposita informativa.

L'Organismo di Vigilanza svolge - con periodicità stabilità dallo stesso – attività di vigilanza su licenziamenti o altre misure adottate dalla Banca (e.g. demansionamenti e trasferimenti) che possano avere natura ritorsiva o discriminatoria nei confronti dei segnalanti.

- *Gestione della segnalazione*

Ricevuta la segnalazione, l'Organismo di Vigilanza, in composizione collegiale, compie un'analisi preliminare volta ad accertare:

- che la segnalazione risulti sufficientemente circostanziata e in ogni caso idonea ad individuare la condotta illecita nonché l'autore della stessa;
- che la condotta denunciata sia rilevante ai sensi del Decreto e del Modello.

Nello svolgimento della suddetta analisi preliminare l'Organismo di Vigilanza potrà avvalersi - per specifici aspetti trattati nelle segnalazioni- del supporto di tutte le funzioni aziendali per quanto di competenza.

L'Organismo di Vigilanza potrà altresì richiedere ulteriori chiarimenti direttamente al segnalante, salvo nel caso di segnalazione anonima, al fine di circostanziare ancor più chiaramente il fatto denunciato e ricercare maggiori fonti di prova afferenti alla condotta contestata e, in primo luogo, per comprendere se la segnalazione è veritiera o pretestuosa.

Le attività di cui sopra saranno espletate attraverso un'indagine tempestiva e accurata, nel rispetto dei principi di imparzialità, equità e riservatezza nei confronti di tutti i soggetti coinvolti.

Qualora a conclusione della fase di analisi preliminare emerga l'assenza di elementi sufficientemente circostanziati o l'infondatezza dei fatti richiamati, la segnalazione sarà archiviata con le relative motivazioni.

Una volta verificata la fondatezza delle segnalazioni ricevute, l'Organismo di Vigilanza potrà sottoporre i risultati alla valutazione delle funzioni della Banca competenti affinché vengano intrapresi i più opportuni provvedimenti, richiedendo – ove opportuno – l'avvio di un procedimento sanzionatorio a carico del soggetto interessato.

Qualora l'Organismo di Vigilanza accerti la malafede del segnalante e/o un suo intento meramente diffamatorio, potrà richiedere l'avvio di un procedimento disciplinare nei confronti del segnalante.

- *Reporting periodico*

L'Organismo di Vigilanza riferisce, nell'ambito delle attività di *reporting*, all'ARC e al Consiglio di Amministrazione sul numero e sulla tipologia di segnalazioni ricevute e ne tiene conto ai fini dell'aggiornamento del Modello. Inoltre, con cadenza almeno annuale l'Organismo di Vigilanza fornisce un *report* riepilogativo delle segnalazioni che gli siano pervenute.

Le risultanze dell'attività istruttoria, delle verifiche effettuate e delle decisioni assunte dall'Organismo di Vigilanza dovranno essere tracciate e archiviate a cura dello stesso.

2.12. Il sistema di comunicazione, informazione e formazione del personale

- *Sistema di comunicazione*

Al fine di divulgare la conoscenza del Modello e del sistema normativo aziendale finalizzato a prevenire la commissione degli Illeciti Rilevanti, l'adozione del Modello e la nomina dell'Organismo di Vigilanza sono comunicate a tutti i Destinatari attraverso specifica circolare interna. Sono inoltre comunicate, di volta in volta, a tutti i Destinatari tutte le variazioni e gli aggiornamenti del medesimo Modello.

Una copia del Modello e della normativa interna al medesimo correlata è, inoltre, pubblicata in una specifica sezione dell'Intranet della Banca dall'Organizzazione Aziendale, accessibili da parte di tutti i Destinatari, in cui sono anche pubblicate tutte le informazioni relative alla nomina dell'Organismo di Vigilanza, circolari e comunicazioni attuative del Modello e ai corsi di formazione organizzati dalla Banca in materia di responsabilità amministrativa degli enti ex D.Lgs. 231/2001.

A tutti i nuovi assunti viene chiesto di prendere visione della normativa aziendale rilevante, che i medesimi sono tenuti a rispettare nello svolgimento delle attività lavorative a favore della Banca (Cfr. Sezione 2.7 della Parte Generale del Modello), tra cui anche il Modello stesso.

- *Sistema di Informazione nei confronti di soggetti esterni alla Banca*

La Banca ha adottato un sistema di selezione dei soggetti esterni alla medesima formalizzato, basato sull'accertamento della sussistenza di specifici requisiti professionali e reputazionali (con particolare riferimento agli EAM", si veda la Norma Operativa N. 2.34 "*Intermediari Finanziari*" e con riferimento ai Procacciatori d'Affari si veda la Norma Operativa N. 2.27)

Al fine di garantire il pieno rispetto della legalità e dei principi etici nell'esercizio delle attività aziendali e dei rapporti d'affari con soggetti terzi, la Banca informa contrattualmente tali soggetti esterni che cooperano con la Banca nell'ambito delle attività sensibili, in merito all'adozione da parte della medesima del presente Modello.

In particolare, la Banca richiede espressamente, attraverso specifica clausola contrattuale, ai soggetti esterni, che cooperano con la Banca nell'ambito delle attività sensibili, di rispettare i principi previsti dalla normativa in materia di responsabilità amministrativa degli enti ex D.Lgs. 231/2001 (anche rispettando il relativo modello organizzativo e di controllo, se esistente) e, ove non abbiano adottato un modello di organizzazione gestione e controllo proprio, di rispettare i principi del Modello 231 adottato dalla Banca stessa che siano ai medesimi applicabili.

L'Organismo di Vigilanza valuterà l'appropriatezza delle clausole contrattuali da proporre ai soggetti esterni, prevedendo, se necessario, clausole diverse a seconda della controparte contrattuale, delle attività eseguite nell'interesse o vantaggio della Banca e, se esistente, del relativo sistema di compliance al D.Lgs. 231/2001 già adottato dalla medesima.

- *Formazione*

Ai fini dell'efficace attuazione del Modello, è obiettivo generale della Banca garantire a tutti i Destinatari la conoscenza delle regole di condotta ivi contenute, degli obiettivi che si intendono perseguire e delle modalità attraverso le quali la Banca ha inteso perseguirli.

In forza di ciò, la Banca inserisce i contenuti del Modello nell'ambito dei propri piani formativi destinati al personale che si occupa di clientela domiciliata in Italia.

Il piano formativo, i cui contenuti sono aggiornati in relazione all'evoluzione normativa interna ed esterna applicabile, viene sottoposto all'Organismo di Vigilanza il quale ne valuta l'efficacia con riferimento ai contenuti, alle modalità di erogazione, alla loro reiterazione, ai controlli sulla partecipazione e alle misure da adottare nei confronti di quanti non partecipino senza giustificato motivo.

La partecipazione ai processi formativi sopra descritti è obbligatoria e sarà oggetto di verifica. I corsi vengono ripetuti con cadenza regolare.

2.13. Adozione, modifiche ed aggiornamento del Modello 231

Il Consiglio di Amministrazione della Banca ha competenza esclusiva per l'adozione e la modificazione del Modello. In particolare, il Consiglio di Amministrazione:

a). provvede a modificare tempestivamente il Modello qualora siano individuate significative violazioni o elusioni delle prescrizioni in esso contenute, che ne evidenziano l'inadeguatezza a garantire l'efficace prevenzione degli Illeciti Rilevanti; e
b). provvede ad aggiornare tempestivamente il Modello, anche su proposta dell'Organismo di Vigilanza, qualora intervengano mutamenti nel sistema normativo o nell'organizzazione e nell'attività della Banca o del Gruppo.

L'Organismo di Vigilanza, in ogni caso, deve prontamente segnalare al Consiglio di Amministrazione eventuali fatti che evidenziano la necessità di revisione del Modello.

PARTE SPECIALE

1. Reati commessi nei rapporti con la Pubblica Amministrazione (Artt. 24 e 25) e reati di corruzione tra privati e di istigazione alla corruzione tra privati (Art. 25-ter, co. 1, lett. s-bis), reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" (Art. 25 decies)

Il presente Capitolo della Parte Speciale si riferisce alle seguenti categorie di reati previste dal D.Lgs. 231/2001:

a). "indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico" di cui all'art. 24 del Decreto;
b). "reati di peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio" di cui all'art. 25 del Decreto;
c). "reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" di cui all'art. 25 decies del Decreto.

Le suddette categorie di reati vengono trattate unitamente nella presente Sezione della Parte Speciale poiché la configurazione delle relative fattispecie presuppone la lesione di interessi della Pubblica Amministrazione e, in alcuni casi, l'instaurazione di rapporti con un pubblico ufficiale o un incaricato di pubblico servizio.

Per affinità di materia e di presidi adottati, si considerano nella presente Sezione anche i reati di corruzione tra privati e di istigazione alla corruzione tra privati di cui agli artt. 2635, co. 3, e 2635-*bis* c.c., richiamati dall'art. 25-ter, co. 1, lett. s-*bis*, del Decreto relativo ai reati societari.

Si fornisce di seguito una descrizione dettagliata delle fattispecie di reati nei confronti della Pubblica Amministrazione previste dagli articoli del Decreto sopra citati, che possono avere rilevanza con riferimento all'attività della Banca.

Ai fini di una più agevole comprensione delle singole fattispecie di reato, si premette che agli effetti della legge penale, si considera ente della Pubblica Amministrazione qualsiasi persona giuridica che persegua e/o realizzi e gestisca interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa, disciplinata da norme di diritto pubblico e manifestantesi mediante atti autoritativi.

Alcune delle fattispecie penali sotto-indicate (ad es., il reato di peculato, concussione e corruzione) presuppongono il coinvolgimento 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. A tal riguardo, si precisa che sono considerati pubblici ufficiali ed incaricati di pubblico servizio tutti coloro che – legati o meno da un rapporto di dipendenza con la Pubblica Amministrazione – svolgono un'attività regolata da norme di diritto pubblico. In particolare:

- pubblico ufficiale è colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa; tale funzione è caratterizzata dalla formazione e dalla manifestazione di volontà della pubblica amministrazione e dal suo svolgersi per mezzo di poteri autorizzativi o certificativi;
- incaricato di pubblico servizio è colui che, come il pubblico ufficiale svolge una pubblica funzione ma a differenza di quest'ultimo, non ha potestà di imperio e di certificazione documentale.

La nozione di pubblico ufficiale o incaricato di pubblico servizio ha, dunque, natura oggettiva, basandosi sull'attività concretamente svolta dal soggetto e non sull'esistenza di un rapporto – contrattuale o di dipendenza – con la Pubblica Amministrazione. Pertanto, è possibile che soggetti, la cui attività è di regola disciplinata dal diritto privato, in taluni settori operino in qualità di pubblici agenti.

Si precisa che ai pubblici agenti italiani sono equiparati tutti coloro che svolgono funzioni analoghe a quelle che ad essi competono nell'ambito di organismi comunitari, di altri Stati membri dell'Unione europea, di Stati esteri o organizzazioni pubbliche internazionali.

1.1. Fattispecie delittuose

1.1.1. Truffa a danno dello Stato e truffa aggravata per il conseguimento di erogazioni pubbliche

Premesso che il reato di truffa ai sensi dell'art. 640 c.p. punisce "*chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sè o ad altri un ingiusto profitto con altrui danno"*. Ai fini del Decreto rilevano le seguenti fattispecie specifiche di truffa:

1. "*truffa a danno dello Stato*" (art. 640, co. 2, c.p.): tale reato si realizza nel caso in cui un soggetto ottenga un ingiusto profitto ponendo in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato, ad altro Ente Pubblico o all'Unione Europea;
2. "*truffa aggravata per il conseguimento di erogazioni pubbliche*" (art. 640-*bis* c.p.): tale fattispecie di reato si configura nel caso in cui sia commesso un reato di truffa ai sensi dell'art. 640 c.p. con riferimento a contributi, sovvenzioni, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, altri enti pubblici o delle Comunità europee.

1.1.2. Frode informatica

La fattispecie di reato, prevista dall'art. 640-*ter* c.p., si realizza nel caso in cui un soggetto, alterando il funzionamento di un sistema informatico o telematico o intervenendo senza diritto sui dati, informazioni o programmi in essi contenuti, procuri a sé o ad altri un ingiusto profitto con altrui danno. Essa assume rilievo ai fini del Decreto, soltanto nel caso in cui sia perpetrata ai danni dello Stato o di altro ente pubblico.

1.1.3. Concussione

La fattispecie di reato, prevista dall'art. 317 c.p., si realizza nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, costringa taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altre utilità.

La costrizione si attua mediante violenza o minaccia di un danno ingiusto (per esempio: rifiuto di compiere un atto dovuto se non contro compenso), con modalità tali da non lasciare libertà di scelta alla persona che la subisce, la quale è considerata vittima del reato e quindi esente da pena. Pertanto, la responsabilità degli enti a titolo di concussione è configurabile, sempre che sussista l'interesse o vantaggio dell'ente, soprattutto nel caso di reato commesso da un soggetto apicale o da un subordinato in concorso con un pubblico ufficiale o un incaricato di pubblico servizio nei confronti di un terzo.

1.1.4. Corruzione (artt. 318 e segg. c.p.)

In generale, il reato di corruzione consiste in un accordo fra un pubblico ufficiale o un incaricato di pubblico servizio e un privato, in forza del quale il primo accetta dal secondo un compenso che non

gli è dovuto per il compimento di un atto contrario ai propri doveri di ufficio (corruzione propria) ovvero conforme a tali doveri (corruzione impropria).

La corruzione si manifesta quando le parti, essendo in posizione paritaria fra di loro, pongono in essere un vero e proprio accordo, diversamente dalla concussione, che invece presuppone lo sfruttamento da parte del soggetto rivestente la qualifica pubblica della propria posizione di superiorità, alla quale corrisponde nel privato una situazione di soggezione. Nel fatto della corruzione si ravvisano due distinti reati: l'uno commesso dal soggetto corrotto, che riveste la qualifica pubblica (c.d. corruzione passiva), l'altro commesso dal corruttore (c.d. corruzione attiva).

Le fattispecie di corruzione rilevanti ai sensi del D.Lgs. 231/2001 sono le seguenti([4]):

- corruzione per un atto d'ufficio (art. 318 c.p.): tale ipotesi si realizza nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio riceva indebitamente, per sé o per o per un terzo, denaro o altra utilità, o ne accetti la promessa, per l'esercizio delle sue funzioni o dei suoi poteri;
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.): tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per omettere o ritardare, o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.
- corruzione in atti giudiziari (art. 319-ter, comma 1, c.p.): in tale fattispecie di reato i fatti indicati negli artt. 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo;
- istigazione alla corruzione (art. 322 c.p.): tale ipotesi di reato si realizza nel caso in cui un soggetto offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, sia qualora l'offerta o la promessa sia accettata sia qualora l'offerta o la promessa non sia accettata.

1.1.5. Corruzione tra privati e istigazione alla corruzione tra privati

L'art. 2635, co. 3, c.c. e l'art. 2635-bis c.c. puniscono la condotta di chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti agli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di altra società o altri soggetti esercenti funzioni direttive (ovvero a chi è sottoposto alla direzione o alla vigilanza di uno di tali soggetti), per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

La pena è ridotta nel caso in cui l'offerta o la promessa non sia accettata (art. 2635-bis c.c.).

1.1.6. Traffico di influenze illecite

Tale ipotesi di reato, prevista dall'art. 346-*bis* c.p., si configura quando un soggetto, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio - o con i soggetti che esercitano corrispondenti funzioni nell'ambito dell'Unione Europea, di Paesi terzi, di Organizzazioni o di Corti internazionali - indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso tali soggetti, ovvero per remunerarli in relazione all'esercizio delle loro funzioni e poteri. La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità.

([4]) Ai sensi dell'art. 320 c.p., le disposizioni degli artt. 318 e 319 c.p. si applicano anche all'incaricato di pubblico servizio.

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

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

1.1.7. Peculato

Tali ipotesi di reato, previste dagli artt. 314 e 316 c.p., si configurano quando:

- un pubblico ufficiale o un incaricato di un pubblico servizio che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria (art. 314 c.p.);
- un pubblico ufficiale o un incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità (art. 316 c.p.).

1.1.8. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri

Ai sensi dell'art. 322 bis c.p., costituiscono reato rilevante ai sensi del Decreto anche i delitti di peculato, concussione, induzione indebita a dare o promettere utilità e istigazione alla corruzione che coinvolgono:

- un membro delle Corti o degli organi delle Comunità europee, nonché a funzionari o agenti delle Comunità europee o coloro che nell'ambito degli Stati Membri della Comunità Europea svolgono funzioni o attività corrispondenti a quelle di pubblico ufficiale o incaricato di pubblico servizio;
- i giudici, procuratori, funzionari e agenti della Corte Penale internazionale e delle corti internazionali, le persone che esercitano funzioni o attività corrispondenti a quelle di pubblico ufficiale e incaricato di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali nonché i membri delle assemblee parlamentari internazionali, di organizzazioni internazionali o sovranazionali;
- le persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione europea.

1.1.9. Indebita percezione di erogazioni pubbliche

Tale ipotesi di reato, prevista dall'art. 316-*ter* c.p., si realizza nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità

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

Secondo l'interpretazione giurisprudenziale, rientrano nel concetto di "erogazioni" ai sensi della fattispecie in esame anche le agevolazioni fiscali.

1.1.10. Abuso d'ufficio

Tale ipotesi di reato, prevista dall'art. 323 c.p., si configura - salvo che il fatto non costituisca un più grave reato - quando un pubblico ufficiale o un incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto.

Ai fini del D.lgs. 231/2001, tale ipotesi di reato rileva solo quando il fatto offende gli interessi finanziari dell'Unione europea.

1.1.11. Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies)

Il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.) (di seguito, per brevità, "*reati di intralcio alla giustizia*"), previsto dall'art. 25-decies del Decreto, è commesso da chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere. Tale fattispecie, qualora commessa con le caratteristiche della transnazionalità, integra anche gli estremi del reato transnazionale ai sensi della legge n. 146/2006 (cfr. Sezione 3 della Parte Speciale del presente Modello).

La norma penale in esame tutela l'interesse al corretto svolgimento dell'attività giudiziaria e mira a prevenire comportamenti in grado di influire negativamente nell'accertamento della verità nel processo penale.

1.2. Attività aziendali sensibili

Il rischio che vengano commessi i reati oggetto della presente Sezione della Parte Speciale è connesso soprattutto allo svolgimento di quelle attività espletate dalle strutture aziendali che siano in relazione diretta o indiretta con soggetti pubblici, ivi inclusi i pubblici ufficiali, gli incaricati di pubblico servizio e le Autorità pubbliche di Vigilanza. Le principali attività aziendali sensibili della Banca identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere reati nei rapporti con la Pubblica Amministrazione e reati di corruzione privata sono le seguenti:

- rapporti con le Pubbliche Autorità (incluse le comunicazioni e/o adempimenti nei confronti di Autorità di Vigilanza e\o di altri Enti Pubblici e nell'ambito di verifiche o accertamenti da parte di Autorità di Vigilanza e gestione di adempimenti fiscali, ove previsti);
- gestione dei procedimenti pendenti davanti alle autorità giudiziarie (es. penali, civili, amministrativi, tributari etc);
- gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni ed eventi promozionali;

- selezione e assunzione del personale;
- selezione dei fornitori e conferimento degli incarichi professionali.

Con riguardo alle attività sensibili sopra individuate, e Unità organizzative principalmente coinvolte nelle attività sensibili sono:

- Consiglio di Amministrazione
- Direzione Generale
- funzione Legal & Compliance ("**L&C**"):
- Risk Management;
- Revisione Interna (Internal Audit);
- Risorse Umane;
- Ufficio Acquisti;
- Responsabile Marketing;
- tutte le Funzioni Proponenti e Funzioni Referenti nell'ambito dei processi di selezione dei fornitori.

1.3. Presidi procedurali e di controllo

L'attività di prevenzione dei reati oggetto del presente Capitolo della Parte Speciale si basa, innanzitutto, sull'adozione di un sistema articolato di misure preventive e di controlli disciplinato nelle policy e procedure interne adottate dalla Banca. In particolare, la Banca ha adottato i seguenti Regolamenti, Policy e Norme Operative rilevanti ai fini della prevenzione dei reati oggetto del presente Capitolo di Parte Speciale del Modello:

- "*Legal & Compliance Policy del Gruppo PKB*"
- "*Regolamento per il personale*";
- "*Procurement Policy*";
- Norma Operativa 4.16 "*conflitto di interessi*";
- Norma Operativa 12.2, recante "*Norma operativa in materia di procurement*";
- Norma Operativa 2.25 recante "*Legal & Compliance Office (L&C)*";
- Norma Operativa 5.60 recante "*Decreti/Ordinanze dell'autorità giudiziaria, lettere di risposta alle autorità*";
- Norma Operativa 5.41 recante "*Pratiche legali*";
- Norma Operativa 4.15 recante "*Assunzione del personale*";
- Norma Operativa 5.8 recante "*Gestione posta banca*";

In particolare, il Regolamento per il Personale prevede il generale divieto di corrompere soggetti terzi, pubblici o privati, così come farsi corrompere da soggetti terzi, pubblici o privati, prevedendo a carico di chiunque ponga in essere tali comportamenti illeciti l'irrogazione di sanzioni disciplinari.

Il Regolamento per il Personale prevede inoltre l'obbligo per tutti i dipendenti che si trovino in una situazione di conflitto di interesse di rispettare la relativa procedura interna per l'attivazione delle funzioni competenti e dei processi di gestione degli stessi. Situazioni di conflitto di interesse possono riguardare tutti gli ambiti di rilevanza della Banca, ed in particolare nei rapporti tra la Banca e un cliente, tra diversi clienti della stessa, tra un membro del personale della Banca e un cliente ovvero la Banca stessa, ovvero anche tra un cliente, un intermediario e la Banca.

Si riporta di seguito una sintesi dei protocolli che dettano i principi di controllo ed i principi di comportamento applicabili alle attività sensibili (e che si completano con le norme operative di dettaglio che regolamentano le attività medesime), che sono funzionali a prevenire i reati di corruzione, nelle loro varie tipologie, nonché i reati di intralcio alla giustizia.

Infine, con particolare riferimento alla prevenzione dei reati di:

- frode informatica, sono ritenuti idonei i principi di controllo e di comportamento individuati nei protocolli inerenti alla prevenzione dei delitti informatici e del trattamento illecito di dati (cfr. Sezione 2 della presente Parte Speciale);
- indebita percezione di erogazione ai danni dello Stato (in particolare, in concorso con la clientela), oltre ai principi di seguito rappresentati e relativi alla gestione dei rapporti con le Pubbliche Autorità, sono ritenuti idonei i principi di controllo e di comportamento individuati nei protocolli inerenti alla prevenzione dei reati societari e tributari (cfr. Sezioni 5 e 8 della presente Parte Speciale).

a. Gestione dei rapporti con le autorità.

La Banca ha adottato regole di comportamento e presìdi volti alla prevenzione di ogni fattispecie corruttiva, sia nei rapporti tra privati, sia nei rapporti con il settore pubblico. In particolare, la Norma Operativa 4.16 sui Conflitti di Interesse prevede:

- il divieto di indurre persone terze o collaboratori a commettere od omettere atti in violazione dei propri obblighi di ufficio, di servizio o di fedeltà offrendo, promettendo o procurando loro qualsiasi tipo di vantaggio;
- il divieto di lasciarsi indurre a commettere od omettere atti in violazione dei propri obblighi di ufficio, di servizio o di fedeltà, facendosi promettere o accettare, per sé, per persone terze o Collaboratori, qualsiasi tipo di vantaggio.

I Destinatari del Modello che venissero a conoscenza di fatti o comportamenti in violazione dei suddetti divieti hanno l'obbligo di segnalarli al Responsabile delle Risorse Umane, che a sua volta provvede ad informare tempestivamente il Chief Risk Officer e il Chief Executive Officer.

La Banca ha individuato nel Chief Executive Officer il soggetto rappresentante della Banca nei rapporti con soggetti terzi e con le autorità pubbliche. In tale ruolo il CEO è coadiuvato dal CRO e dal CFO.

Con particolare riferimento alla corrispondenza scritta tra la Banca e soggetti terzi, in particolare, le autorità pubbliche, sono stati adottati i seguenti presidi:

- tutta la corrispondenza in entrata è debitamente registrata, protocollata e trasmessa da parte dei "Servizi Vari" agli uffici interessati;
- tutta la corrispondenza destinata ai membri della Direzione Generale (tra cui il Chief Executive Officer), Legal & Compliance, Risorse Umane e Revisione Interna è censita in un apposito registro (c.d. "*registro raccomandate e corrispondenza con valori*"), indicante: data di ricezione, mittente, breve descrizione del contenuto e l'eventuale importo valori;
- il CRO e il CFO supportano il CEO nell'analisi delle richieste e delle comunicazioni da inviare alle Autorità Pubbliche nonché nella predisposizione delle relative lettere di risposta, affinché sia garantita la massima coerenza e conformità alle disposizioni normative e regolamentari vigenti;

- tutta la corrispondenza con le autorità pubbliche è sottoscritta da due membri della Direzione Generale;
- tutta la corrispondenza con le autorità pubbliche in uscita, inclusa la corrispondenza con le autorità pubbliche, è riprodotta in formato digitale e protocollata e archiviata nell'archivio di riferimento dopo l'apposizione delle firme sul documento.

Con riferimento agli incontri di persona tra il personale della Banca e le autorità pubbliche, la Banca adotta le seguenti misure:

- la Banca ha individuato nel CEO, CRO e CFO i soggetti generalmente competenti ad accogliere ed interfacciarsi con i funzionari pubblici nel corso di incontri istituzionali, ispezioni, audizioni etc. La Direzione Generale può accordare singole deleghe qualora in specifiche situazioni si rendesse necessaria la presenza di ulteriori funzioni.
- a tutti gli incontri con funzionari delle autorità pubbliche partecipano almeno due dipendenti della Banca;
- tutti gli incontri con funzionari delle autorità pubbliche sono verbalizzati per iscritto in documenti che vengono conservati a cura della Segreteria della Direzione Generale.

b. Gestione dei procedimenti pendenti davanti alle autorità giudiziarie

La Banca ha adottato la Norma Operativa 5.60 per la gestione di "*Decreti /Ordinanze dell'autorità giudiziaria, lettere di risposta all'autorità*". In particolare, la suddetta norma operativa prevede le seguenti misure atte a prevenire potenziali illeciti connessi al corretto svolgimento dell'attività giudiziaria:

- tutti gli ordini e le comunicazioni delle autorità giudiziarie svizzere o estere sono presi in carico e gestiti dalla funzione L&C;
- gli ordini e le comunicazioni delle autorità giudiziarie che comportano rischi finanziari, di compliance o reputazionali rilevanti sono trasmessi anche al CRO;
- La funzione L&C verifica che le richieste siano legittime, giustificate e meritevoli di risposta da parte della Banca;
- La funzione L&C avvia i processi di controlli interni opportuni e necessari al fine di evadere le richieste delle autorità giudiziarie. A tal riguardo sono stati adottati specifici processi interni per l'evasione sia delle risposte negative, sia delle risposte positive;
- La funzione L&C assicura che tutte le risposte elaborate per conto della Banca siano esaurienti e veritiere, ossia che rispecchino, sotto tutti i punti di vista, il vero stato delle cose, sia che si tratti di risposte affermative, sia che si tratti di risposte negative;
- La funzione L&C riporta trimestralmente al CRO eventuali casi meritevoli di attenzione per una corretta gestione dei rischi di compliance e reputazionali

Ove necessario, la Banca nomina dei legali esterni per la propria difesa in giudizio. A tal riguardo, è stata adottata la Norma Operativa 5.41 "*Pratiche Legali*" che individua nel L&C la funzione competente a gestire le pratiche legali e nel CRO il soggetto competente ad approvare preventivamente, ove necessario, la nomina di legali esterni.

c. Gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni ed eventi promozionali

Il Regolamento per il Personale vieta espressamente a tutti i dipendenti della Banca di:

- offrire o promettere benefici a terzi per ottenere un vantaggio da parte loro;
- accettare, per sé stesso, per i suoi congiunti o persone vicine, alcun compenso in denaro o regalo impegnativo o farsi promettere o accordare altri favori (ad esempio lasciti). In caso di offerte di compenso il Dipendente è tenuto ad informare immediatamente il proprio superiore diretto.

In particolare, in relazione ai benefici a favore di soggetti terzi, sono stati adottati i seguenti presidi in materia di: i) omaggi e liberalità; ii) beneficienza; sponsorizzazioni ed eventi promozionali; iii) rimborsi spese e spese di rappresentanza

1) Con riferimento agli omaggi e alle liberalità a favore di soggetti terzi sono stati adottati i seguenti presidi:

- gli omaggi e le liberalità nei confronti di soggetti terzi sono generalmente ammessi nell'ambito delle comuni prassi commerciali e di cortesia (a titolo esemplificativo in occasione delle festività natalizie) e comunque entro valori contenuti;
- gli omaggi e le liberalità a favore di soggetti terzi possono essere scelti tra i beni elencati in un catalogo predefinito, curato dal Responsabile Marketing;
- eventuali regali occasionali, al di fuori del catalogo tenuto del Responsabile Marketing e di importo superiore alla media dei regali e liberalità, sono approvati dal responsabile di linea del richiedente e dal Responsabile Marketing, nei limiti del budget pre-assegnato all'ufficio del richiedente;
- le richieste di omaggi e liberalità a favore di soggetti terzi, anche a titolo di beneficienza, sono formalizzate attraverso l'invio di un email specifica al responsabile Marketing;
- il Responsabile Marketing valida le richieste di acquisto di omaggi e liberalità, previa verifica del rispetto del budget di spesa assegnato al richiedente / all'ufficio del richiedente;
- il Responsabile Marketing conserva tutte le richieste di fornitura di beni a scopo di omaggi e liberalità;

2) Con riferimento al rimborso delle spese ai dipendenti, la Banca ha adottato delle procedure interne, tra cui in particolare il Regolamento sulle "*Spese di rappresentanza, promozionali, viaggi di lavoro e di formazione*" che prevedono quanto segue:

- la Banca rimborsa ai propri dipendenti esclusivamente le spese dai medesimi anticipate per l'espletamento dell'attività lavorativa a favore della Banca;
- le richieste di rimborso spese, formulate tramite moduli standard (nei quali sono richiesti informazioni e documenti giustificati relativi alle spese sostenute), sono sottoposte all'approvazione del responsabile di linea e alla validazione da parte dell'Ufficio contabilità, che verifica la correttezza e completezza della documentazione giustificativa;
- al personale dirigente è consentito effettuare spese di rappresentanza, che hanno l'obbiettivo di facilitare lo sviluppo degli affari e/o promuovere pubbliche relazioni che siano di beneficio per la Banca, purché le medesime siano debitamente documentate (con scontrino o fattura) e approvate in conformità alle norme operative aziendali; .

3) con riferimento alle sponsorizzazioni e agli eventi promozionali, considerato che si tratta di attività sporadica, la Banca segue la seguente prassi:

- tutti i progetti di sponsorizzazione e gli eventi promozionali sono autorizzati dal Responsabile Marketing sulla base di richiesta scritta;
- l'approvazione di progetti di sponsorizzazione e/o eventi promozionali è soggetta a controlli sul rispetto del budget assegnato alla funzione richiedente.

4) Con riferimento ad omaggi e liberalità offerti ai Destinatari, la Norma Operativa 4.16 "*Conflitti di Interesse*" prevede le seguenti misure atte a prevenire fenomeni di tipo corruttivo, sia pubblici che privati:

- i Destinatari possono accettare da soggetti terzi esclusivamente regali di valore commerciale trascurabile non superiori a CHF 100 (o controvalore);
- benefici o omaggi di valore superiore a CHF 100 da parte di Clienti o fornitori non devono essere accettati dai Destinatari, salvo che il Destinatario, accettandoli, abbia la possibilità di contraccambiare personalmente o a spese Banca presentando un giustificativo spese. Tali benefici devono comunque essere comunicati al superiore diretto;
- eventuali donazioni o altri lasciti da parte di un cliente a favore di un Destinatario devono essere autorizzati da un membro della Direzione Generale, il quale deve comunque informare il CEO;
- ogni Destinatario che nota fatti e comportamenti in violazione dei suddetti presidi ha l'obbligo di segnalarlo immediatamente al responsabile delle Risorse Umane che provvederà a informare il CRO e il CEO.

d. Processo di assunzione del personale

La Banca potrebbe essere esposta al rischio che siano commesse la fattispecie di reato in esame nell'ambito dei processi di selezione finalizzati all'assunzione di collaboratori (ad es. nell'ambito dei processi in oggetto potrebbero essere offerte posizioni lavorative a soggetti raccomandati da pubblici ufficiali o incaricati di pubblico servizio al fine di ottenere favori da questi ultimi).

In particolare, la Banca ha adottato la Norma Operativa 4.15 "*Assunzione di Personale"* volta a definire i presupposti, le attività e le responsabilità della ricerca, selezione ed assunzione di Collaboratori. In tale contesto sono state adottate le seguenti misure atte a prevenire fenomeni corruttivi:

- il responsabile dell'unità organizzativa che necessita di nuove risorse deve trasmettere alle Risorse Umane una richiesta di assunzione di personale, debitamente documentata, motivata e recante indicazione del profilo professionale che il nuovo Collaboratore deve possedere;
- l'ufficio Risorse Umane verifica la sostenibilità economica della nuova assunzione rispetto al budget dell'unità organizzativa richiedente e trasmette la documentazione al CEO, il quale decide in merito all'avvio del processo di assunzione;
- il processo di ricerca del nuovo collaboratore è curato dalla funzione Risorse Umane che provvede (i) dapprima a ricercare potenziali candidati internamente alla Banca stessa e (ii) ove non fosse possibile ricoprire la posizione dall'interno, ad avviare la ricerca tramite canali esterni;
- la funzione Risorse Umane provvede alla raccolta della documentazione, ad una prima verifica sui candidati (es. World-check, internet, ecc.) nonché alla trasmissione all'unità organizzativa richiedente delle candidature maggiormente aderenti al profilo richiesto;
- il candidato viene selezionato in base ad una sequenza di colloqui tenuti con almeno tre rappresentanti della Banca. Ogni intervistatore riporta il risultato dell'incontro su un apposito formulario da cui risulta chiaramente l'eventuale raccomandazione di assunzione;
- la funzione Risorse Umane prima dell'assunzione effettua controlli supplementari ("background check") sui candidati e sulle relative referenze.

L'assunzione di persone che rivestono funzioni di rappresentanza, amministrazione, direzione e controllo (CEO, membri della Direzione Generale, direttori, condirettori, vicedirettori, ecc.) avviene secondo specifici processi che stabiliscono i soggetti responsabili della proposta di assunzione, quelli responsabili dell'approvazione, nonché i soggetti cui è dovuta informativa in merito all'assunzione

stessa. In particolare, l'assunzione e il licenziamento del personale con qualifiche più elevate sono sottoposti a processi autorizzativi gradatamente più strutturati a seconda dell'importanza gerarchica del ruolo da ricoprire, sino a coinvolgere - dal livello di direttore a salire - il comitato nomine e remunerazioni per la relativa validazione.

e. Selezione dei fornitori e conferimento degli incarichi professionali.

La Banca potrebbe essere esposta ai reati in esame in relazione ai processi di selezione e di formalizzazione di rapporti contrattuali con controparti e *outsourcer* (ad esempio, ove la selezione sia effettuata su raccomandazione di pubblici ufficiali o incaricati di pubblico servizio al fine di ottenere da questi ultimi favori o vantaggi).

La Banca ha adottato la Procurement Policy e la Norma Operativa n. 12.2. "*Norma Operativa in materia di procurement"* che disciplina le modalità di selezione, contrattualizzazione nonché supervisione dei fornitori e degli *outsourcer*. In particolare, la Procurement Policy, approvata dalla Direzione Generale:

- stabilisce i principi e le regole sulla base dei quali è strutturato l'intero sistema di selezione e gestione dei fornitori di beni e servizi. In particolare, il sistema di procurement è basato sui seguenti Principi Generali: 1) etica e legalità, 2) economicità, 3) trasparenza e controllo; 4) ownership e accountability, 5) gestione dei rischi; 6) sicurezza e confidenzialità;
- definisce specifici ruoli e responsabilità, a diversi livelli organizzativi, nell'ambito dello svolgimento delle seguenti attività:
    - la definizione delle strategie di approvvigionamento outsourcing e internalizzazione più idonee a soddisfare le esigenze organizzative ed operative della Banca (in capo alla Direzione Generale e al Consiglio di Amministrazione);
    - la formulazione di richieste di approvvigionamento (c.d. "*Funzione Proponente*");
    - la gestione delle richieste di approvvigionamento, tramite la selezione di fornitori, la gestione degli accordi contrattuali, il censimento delle forniture e degli outsourcing attivi, il monitoraggio della conformità della fornitura rispetto alla Procurement Policy e alla Norma Operativa di attuazione (in capo all'Ufficio Acquisti);
    - la definizione dei rischi derivanti da outsourcing critici e la definizione delle azioni di mitigazione necessarie (in capo alla funzione Risk Management);
    - la negoziazione e definizione di accordi contrattuali, nel rispetto della normativa tempo per tempo applicabile (in capo alla funzione L&C);
    - il monitoraggio dell'operato del fornitore e dei rapporti continuativi in essere tramite la gestione degli aspetti operativi contrattuali, la definizione, l'analisi e il monitoraggio di Key Performance Indicators, nonché attraverso la gestione dei flussi informativi da e verso il fornitore e l'autorizzazione al pagamento in coerenza con i termini contrattuali pattuiti (c.d. "*Funzione Referente*");
    - la contabilizzazione e il pagamento delle forniture di beni e servizi (in capo all'Ufficio Accounting);
- definisce le principali fasi e le relative linee guida per la gestione dei processi di selezione, acquisto ed outsourcing, la cui applicazione è dettagliata nella Norma Operativa 12.2. "*Norma Operativa in materia di procurement*".

Ai fini della prevenzione dei reati in oggetto, sono previste le seguenti misure:

- l'intero processo di selezione e ingaggio dei fornitori esterni è suddiviso per fasi, che coinvolgono diverse funzioni aziendali e prevedono processi diversificati a seconda della rilevanza dell'attività e del valore dei beni o dei servizi che si intende richiedere al fornitore esterno;
- tutte le richieste di fornitura o di outsourcing sono formalizzate per iscritto dalla Funzione Proponente, la quale deve, a seconda dei casi, (i) svolgere un'analisi preliminare della fornitura o dell'esternalizzazione o (ii) per progetti con impatti critici sulla Banca e/o di valore rilevante, predisporre uno studio di fattibilità. In quest'ultimo caso, la predisposizione dello studio di fattibilità può avvalersi del supporto dell'Ufficio Acquisti, Risk Management ed eventualmente del Gruppo Organizzazione e Progetti;
- tutti i nuovi fornitori sono sottoposti ad una classificazione del relativo rischio di impatto sull'operatività aziendale, al fine di adottare adeguate misure di mitigazione sia in fase contrattuale, sia in fase di esecuzione del rapporto contrattuale stesso;
- per gli acquisti e le forniture, di fornitori non classificati come out-of-scope, di importo superiore a CHF 20.000, l'identificazione dei potenziali fornitori, a cui inviare una richiesta di offerta ("Request for Proposal"), è demandata all'Ufficio Acquisti con il coinvolgimento della Funzione Proponente. Eccezioni sono previste dove giustificate da criteri esplicitati nella norma stessa (e.g. per motivi strategici definiti dalla Direzione Generale, vincoli di mercato);
- l'individuazione dei fornitori avviene sulla base di criteri predeterminati, ossia: a) le competenze e le capacità tecniche e professionali del fornitore, b) la struttura organizzativa c) il possesso di tutte le autorizzazioni richieste dalla normativa vigente e attestanti la professionalità e affidabilità del fornitore, d) l'adozione di requisiti di sicurezza logica e fisica che dovranno essere garantiti nell'esecuzione della prestazione;
- per ogni fornitura di valore economico superiore a CHF 20'000 è prevista la richiesta di almeno tre offerte da parte di diversi fornitori al fine di effettuare una valutazione comparativa. Eventuali eccezioni a tale principio devono essere specificate per iscritto dalla Funzione Proponente all'Ufficio Acquisti e approvate espressamente dalla Direzione Generale. La Direzione Generale può disporre di acquisti senza richiesta di offerta a più fornitori in casi particolari (e.g. per motivi strategici);
- la valutazione delle offerte ricevute è effettuata congiuntamente dalla Funzione Proponente e dall'ufficio Acquisti. L'esito di tale valutazione è formalizzato in un documento scritto che viene sottoposto al Capo Divisione per le opportune valutazioni o, in caso di coinvolgimento di più divisioni, al COO e da quest'ultimo alla Direzione Generale per l'approvazione;
- all'esito della selezione, per tutti i fornitori classificati non come Comuni e non "Out-of-scope",, la Funzione Proponente predispone una "Richiesta di Acquisto", controfirmata dall'Ufficio Acquisti e approvata nel rispetto del principio dei "quattro occhi" dal COO o dal CEO;
- tutte le forniture di beni e servizi, di qualsiasi valore, sono formalizzate in accordi contrattuali, i cui contenuti sono più o meno vincolanti a seconda della rilevanza della fornitura;
- tutta la documentazione contrattuale relativa alla fornitura dei servizi è archiviata a cura dell'Ufficio Acquisti a meno di specifiche deroghe per cui vengono archiviate dalla Funzione referente;
- le forniture di beni e servizi sono sottoposte a specifici processi di monitoraggio, più o meno intensi a seconda della rilevanza della fornitura, che consistono in controlli dell'erogazione dei beni e servizi, nella verifica della reportistica di controllo e nell'incontro periodico con i referenti del fornitore;

- tutte le fatture ricevute dai fornitori sono soggette a specifici processi di controllo e di autorizzazione che coinvolgono diverse funzioni, uffici e soggetti, a seconda del grado di rilevanza della fornitura;
- il pagamento delle fatture avviene solo a seguito di autorizzazione da parte delle funzioni competenti.

2. Reati informatici (art. 24-bis)

Con la legge 18 marzo 2008, n. 48 ("Legge 48/2008"), di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, è stato riformato il codice penale in tema di reati informatici, sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti.

La stessa Legge 48/2008 ha introdotto nel Decreto il nuovo art. 24-bis, che prevede la responsabilità amministrativa degli enti per un elenco specifico di reati informatici.

Tenuto conto che i reati informatici possono essere realizzati con modalità tali da rendere difficile l'identificazione del soggetto persona fisica che ha materialmente posto in essere la condotta, si ricorda che ai sensi dell'art. 8 del Decreto la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato.

Si fornisce di seguito una descrizione dettagliata delle fattispecie dei reati informatici considerate rilevanti ai fini del presente Modello, tenuto conto della particolare operatività della Banca.

2.1. Fattispecie delittuose

2.1.1. Acceso abusivo ad un sistema informatico o telematico

Ai sensi dell'art. 615-ter c.p., commette reato chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La norma è posta a tutela del c.d. domicilio informatico, prescinde dalla natura personale dei dati contenuti nel sistema e abbraccia, più in generale, il diritto del titolare di escludere terzi dalla propria sfera privata. Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema.

Nel contesto di operatività della Banca, il reato può essere commesso, ad esempio, nell'ipotesi in cui un Collaboratore acceda, nell'interesse o a vantaggio della Banca, nel sistema informatico di un soggetto terzo al fine di acquisirne abusivamente le informazioni ivi contenute.

2.1.2. Falsità in un documento informatico pubblico o privato avente efficacia probatoria

L'art. 491-bis c.p. dispone la punibilità in relazione ai reati di falsità in atti, previsti dal Capo III, Titolo VII, Libro II, che riguardino documenti informatici pubblici aventi efficacia probatoria. Il riferimento è, in particolare, ai reati di falsità materiale o ideologica commessa dal privato e uso di atto falso.

A tal fine, per "documento informatico" deve intendersi "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", in conformità a quanto previsto dall'art. 1, lett. p), del decreto legislativo 7 marzo 2005, n. 82 (c.d. "Codice dell'amministrazione digitale").

Nei reati di falsità in atti l'ordinamento distingue tra le falsità materiali e le falsità ideologiche: la prima si concretizza nella condotta diretta a modificare una realtà documentale preesistente rispetto a quella che l'autore del falso fa apparire; la falsità ideologica consiste in quella condotta tesa a redigere un documento, che quindi è genuino e proviene realmente da chi appare esserne l'autore, il cui contenuto, però, non corrisponde al vero.

Nel contesto di operatività della Banca, il reato può essere commesso, ad esempio, da un Collaboratore che, mediante l'utilizzo di firma elettronica altrui, modifichi un documento informatico avente valore legale.

Si ricorda che l'art. 640- ter c.p. punisce il delitto di frode informatica perpetrata ai danni dello Stato o di altro ente pubblico. Tale fattispecie costituisce un reato presupposto della responsabilità amministrativa degli enti ai sensi dell'art. 24 del Decreto (cfr. Sezione 1.1.2 della Parte Speciale del Modello).

2.2. Attività aziendali sensibili

Considerato l'utilizzo dei sistemi informatici a tutti i livelli aziendali, il rischio di commissione di reati informatici è, potenzialmente, correlato a tutte le attività aziendali svolte attraverso l'ausilio di strumenti informatici e interessa quindi tutti i Collaboratori della Banca e in generale i Destinatari del Modello.

Nello specifico, le principali attività aziendali sensibili che espongono la Banca al rischio di commissione di tali fattispecie di reato sono quelle svolte dalle strutture aziendali della Banca che, nell'espletamento delle attività di propria competenza, utilizzano e/o gestiscono strumenti, sistemi e programmi informatici (gli "**Strumenti ICT**") che compongono l'infrastruttura informatica della Banca (il "**Sistema ICT**"), nonché quelle che gestiscono, custodiscono, ricevono e trasmettono a soggetti terzi documenti e dati informatici della Banca. In via meramente esemplificativa si menzionano le seguenti attività aziendali sensibili:

a) definizione e gestione del Sistema ICT;
b) installazione e gestione di hardware e software;
c) gestione dei server della rete aziendale e della posta elettronica;
d) gestione e controllo degli accessi ai sistemi informatici;
e) gestione dei dati e dei documenti informatici.

Con riguardo alle fattispecie delittuose sopra individuate, le unità organizzative della Banca principalmente coinvolte sono:

- Consiglio di Amministrazione;
- Direzione Generale;
- Funzione Sicurezza;
- Gruppo Funzione ICT;
- Revisione Interna;
- Funzione Legal & Compliance;
- Risorse Umane;
- Responsabili delle funzioni di business;

2.3. Principi di controllo e di comportamento e protocollo aziendale

Si riporta di seguito una descrizione dei presidi procedurali e di controllo adottati dalla Banca al fine di prevenire la commissione dei reati oggetto della presente Sezione di Parte Speciale del Modello. Tali presidi si sostanziano in un sistema articolato di misure preventive e di controlli, formalizzate in apposite Policy e Norme Operative, nell'ambito delle quali sono definiti in modo chiaro e specifico i diversi ruoli e responsabilità.

In particolare, i suddetti presidi sono formalizzati nelle seguenti Policy e Norme Operative interne:

- Politica in materia di sicurezza del Gruppo PKB (la "**Politica di Sicurezza**");
- Norma Operativa 11.1 recante "Gestione degli accessi applicativi";
- Norma Operativa 11.2 recante "Classificazione e trattamento delle informazioni e regole sulla privacy";
- Norma Operativa 11.3 recante "Clean desk e clear screen";
- Norma Operativa 11.4 recante "Gestione degli incidenti";
- Norma Operativa 11.5 recante "Gestione dei cambiamenti informatici";
- Norma Operativa 11.6 recante "Gestione dei backup";
- Norma Operativa 11.7 recante "Assegnazione dei dispositivi mobili aziendali";
- Norma Operativa 11.8 recante "Business Continuity Plan";
- Norma Operativa 11.9 recante "Sicurezza delle comunicazioni";
- Norma Operativa 11.11 recante "Gestione del rischio informatico";

Di seguito si riportano i presidi che la Banca adotta in relazione alle diverse attività aziendali sensibili al fine di garantire un elevato livello di sicurezza informatica e prevenire la commissione dei reati oggetto della presente Sezione di Parte Speciale.

a. Definizione e gestione del Sistema ICT

La Banca ha identificato il "*rischio informatico*" come uno dei rischi rientranti nell'ambito del "*Rischio Operativo*" contemplato nel Risk Appetite Framework Policy di Gruppo. La gestione del rischio informatico trova concreta espressione nella determinazione di un efficace quadro normativo interno, nella relativa applicazione, nonché in un'adeguata organizzazione aziendale.

In particolare, la banca ha adottato la Policy recante "Politica in materia di sicurezza del Gruppo PKB" (c.d. "Politica di Sicurezza"), che:

1) definisce i principi che guidano la definizione e implementazione dei sistemi di sicurezza informatica di tutte le società del Gruppo, tra cui la Banca stessa,
2) Identifica gli standard e le metodologie a cui le società del Gruppo, tra cui la Banca, devono ispirarsi nella definizione delle infrastrutture informatiche;
3) descrive i ruoli e le responsabilità degli organi e delle funzioni coinvolte nei processi IT;
4) individua le linee guida per un'adeguata gestione della sicurezza informatica a tutti i livelli aziendali e in relazione all'intera infrastruttura informatica, che la Banca ha implementato tramite l'emanazione di apposite Norme Operative.

Nello specifico, al fine di assicurare la protezione del proprio patrimonio informatico, la Banca si attiene ai seguenti principi sanciti nella Politica di Sicurezza:

- riservatezza: le informazioni possono essere fornite solo al personale autorizzato a riceverle;
- integrità: le informazioni devono essere accurate, complete ed elaborate secondo *standard* di qualità costanti che consentano di verificare l'integrità dei dati in qualsiasi fase del processo di elaborazione;
- disponibilità: le informazioni devono essere disponibili quando necessario;
- verificabilità (tracce di riferimento per la revisione): l'elaborazione elettronica dei dati deve poter essere ricostruita sulla base di registrazioni automatiche delle informazioni (es. log), in modo da consentire di verificare la validità delle fonti d'informazione e delle modifiche effettuate;

- documentazione: i dettagli concernenti lo scopo e il livello delle misure di protezione delle informazioni implementate devono essere documentati in modo chiaro;
- aggiornamento: la Politica di Sicurezza deve essere costantemente rivista, aggiornata e adattata in funzione dei cambiamenti intervenuti in ambito normativo, tecnologico e organizzativo.

La Politica di Sicurezza prevede che tutte le società del Gruppo PKB, inclusa la Banca, adottino una politica in materia di sicurezza informatica e un sistema di Norme Operative coerenti con le linee guida stabilite dalla Politica di Sicurezza stessa nonché gli standard e le metodologie ivi previste.

Inoltre, la Politica di Sicurezza definisce i ruoli e le responsabilità attribuiti agli organi, ai comitati interni e alle unità organizzative della Banca al fine assicurare - in osservanza ai principi sopra richiamati - un'efficacie prevenzione dei reati oggetto della presente Sezione di Parte Speciale. Le Norme Operative elaborate dalla Banca definiscono ulteriori compiti e responsabilità degli organi e delle unità organizzative della Banca stessa.

Con riferimento all'organizzazione aziendale, la Banca ha istituito:

- la Funzione Sicurezza, a cui è attribuito il compito di assicurare l'applicazione dei principi di sicurezza definiti dal Consiglio di Amministrazione e dalla Direzione Generale;
- la Funzione ICT, che contribuisce alla definizione delle linee guida aziendali della sicurezza informatica e all'applicazione delle stesse.

Inoltre, considerato l'utilizzo diffuso a tutti i livelli aziendali degli strumenti informatici e telematici, la Banca ha previsto che tutti i Collaboratori siano contrattualmente obbligati a:

- utilizzare gli strumenti informatici in conformità agli usi espressamente consentiti,
- rispettare le misure di sicurezza informatiche adottate dalla Banca,
- garantire la riservatezza delle informazioni anche una volta terminato il rapporto di lavoro.

La Banca promuove iniziative volte a garantire un'adeguata formazione dei Collaboratori sulle tematiche attinenti alla sicurezza informatica e sugli eventuali aggiornamenti in materia.

La Banca ha elaborato un'apposita Norma Operativa (cfr. Norma Operativa 11.11 recante "Gestione del rischio informatico") che formalizza i diversi presidi e le contromisure dalla stessa implementati al fine di far fronte ai diversi scenari di rischio informatico, insiti nel sistema informatico stesso della Banca o dal relativo utilizzo da parte dei Collaboratori.

Al fine di verificare la sicurezza del Sistema ICT, la Banca commissiona ad esperti esterni l'esecuzione di attività di Vulnerability Assessment e Penetration Test sul sistema informatico aziendale, da eseguirsi periodicamente (di principio annualmente), definendone di volta in volta il perimetro. Tali attività permettono di eseguire una verifica periodica della sicurezza del sistema informatico, nonché di individuare efficaci contromisure rispetto alle nuove minacce individuate. La definizione del perimetro da sottoporre a tali attività è effettuata dalla Funzione ICT. La Banca si avvale inoltre di un Security Operation Center (SOC) che dall'esterno monitora ed allerta in caso di anomalie nel sistema informatico.

b. Installazione e gestione di hardware e software

L'acquisto, la gestione e la manutenzione degli strumenti hardware e software che compongono il Sistema ICT sono gestiti dalla Funzione ICT, o laddove necessario in coordinamento con altri uffici (i.e. Ufficio Acquisti, Gruppo Organizzazione/Progetti).

Con riferimento all'acquisto di software e hardware informatici (anche derivante da esigenze di cambiamenti informatici), la Banca ha adottato uno specifico processo di presa in carico delle

richieste e approvazione delle stesse, che coinvolge diversi organi e funzioni aziendali (in particolare l'Ufficio Acquisti e il Comitato Progetti sotto la responsabilità del COO, la cui composizione varia a seconda dell'area interessata dal cambiamento informatico e comunque prevede sempre il coinvolgimento del Responsabile Gruppo ICT).

Con riferimento all'implementazione di nuovi software e hardware è previsto lo svolgimento di preventivi test di verifica (in "ambiente di test" ed in "ambiente di collaudo") sulla compatibilità del nuovo prodotto con il Sistema ICT della Banca e le misure di sicurezza dalla medesima adottate in modo tale da non compromettere la funzionalità del sistema informatico stesso della Banca.

La Banca effettua, inoltre, ulteriori verifiche sui nuovi software/hardware acquistati, sulle eventuali nuove versioni rilasciate e sulle patch di sicurezza al fine di vagliare:

- la presenza di virus o altro codice malevolo sui supporti di memorizzazione utilizzati;
- la compatibilità con il sistema informatico aziendale;
- l'assenza di falle di sicurezza (vulnerabilità).

Tutti gli Strumenti ICT (software e hardware) sono classificati in un apposito inventario tenuto ed aggiornato dalla Banca.

Non è consentito ai Collaboratori di acquistare e installare, in proprio, Strumenti ICT non autorizzati. Anche l'installazione di hardware e software gratuiti è subordinata all'autorizzazione specifica di un amministratore di sistema.

c. Gestione dei server, della rete aziendale e della posta elettronica

La rete aziendale della Banca è configurata in modo tale da consentire l'accesso esclusivamente al personale della Banca in possesso delle necessarie autorizzazioni e credenziali di accesso (infra par. d. "*Gestione e controllo degli accessi ai sistemi informatici*", della presente Sezione).

L'utilizzo della rete Internet aziendale e della posta elettronica aziendale è consentito esclusivamente per uso lavorativo da parte dei soli Collaboratori della Banca, ovvero da parte di altri soggetti specificamente autorizzati.

Con riferimento all'utilizzo di Internet la Banca ha adottato i seguenti presidi:

- è stato disabilitato il *download* di programmi e altre componenti installabili;
- è stato bloccato l'accesso a siti considerati non sicuri;
- è stato bloccato l'accesso a risorse *web mail* di fornitori esterni;
- è stato bloccato l'accesso a siti che permettono l'upload di dati;
- il *download* di documenti è consentito solo per specifici formati e attraverso il *browser* selezionato dalla Banca;
- le attività di accesso ad Internet e consultazione sono registrate per consentire il controllo del corretto utilizzo dei sistemi informatici aziendali.

Tutte le postazioni con un accesso alla rete Internet aziendale sono dotate di software antivirus e/o di meccanismi di sicurezza idonei a proteggere i Sistemi ICT della Banca dal rischio di attacchi informatici o virus.

I clienti della Banca possono utilizzare esclusivamente una rete *Wi-Fi* appositamente predisposta dalla Banca ed autonoma rispetto ai sistemi informatici aziendali.

Infine, la Banca è dotata di sistemi per l'archiviazione dei messaggi di posta elettronica che, ai fini di controllo, consentono l'accesso alle informazioni ivi contenute da parte della Revisione Interna.

d. Gestione e controllo degli accessi ai sistemi informatici

Le modalità di accesso logico e fisico alle varie componenti del Sistema ICT (ivi compresa l'assegnazione di dispositivi mobili aziendali) rispettano i seguenti principi guida:

- *Need-to-know*: il perimetro di accesso conoscitivo alle informazioni è limitato a quanto necessario per lo svolgimento dei compiti assegnati. Compiti e ruoli diversi implicano profili di accesso diversi.
- *Need-to-use*: il perimetro di accesso operativo alle informazioni è limitato a quanto necessario per lo svolgimento dei compiti assegnati. Compiti e ruoli diversi implicano profili di accesso diversi.

Con riferimento all'accesso logico al Sistema ICT, la Banca consente l'accesso solo attraverso l'utilizzo di utenze, a cui sono assegnate credenziali univoche, create dalla Banca ed assegnate ai Collaboratori secondo procedure formalizzate. In particolare, la gestione del ciclo di vita delle utenze e la profilazione degli accessi prevede le seguenti attività:

- creazione delle utenze ed identificazione degli applicativi a cui dare accesso in base alla profilatura dell'utente;
- gestione dei profili applicativi tramite assegnazione di un profilo di autorizzazione (c.d. privilegi) in linea con le mansioni assegnate e secondo il principio di "minimo privilegio". È fatta salva la concessione di deroghe opportunamente documentate;
- modifica dei profili e dei privilegi in caso di variazione del ruolo ricoperto dal Collaboratore nell'organizzazione della Banca;
- disabilitazione delle utenze nel caso in cui il Collaboratore non abbia più necessità di utilizzarle a seguito di cambiamenti delle proprie mansioni lavorative, in casi di assenza prolungata o cessazione del rapporto di lavoro;
- monitoraggio e verifica periodica (almeno annuale) delle utenze e dell'adeguatezza dei profili abilitativi assegnati da parte della Funzione Sicurezza.

La Banca ha implementato specifiche misure relative all'accesso logico al Sistema ICT e alla protezione di tali accessi che, in particolare, consistono:

- in un sistema di autentificazione che richiede l'inserimento di nome utente e password (assegnati in modo univoco a ciascun utente ed elaborati secondo specifici criteri di sicurezza) e per profili che richiedono un maggiore livello di sicurezza, l'utilizzo di strumenti di *strong authentication* (es. *token/ PIN*);
- nella scadenza periodica delle password assegnate a ciascun profilo e l'obbligo dei Collaboratori di aggiornare le password scadute;
- nella registrazione delle informazioni relative agli accessi in appositi "*log*" a ciò dedicati, in modo da consentirne la consultazione ai fini di controllo, monitoraggio e tracciatura degli accessi al Sistema ICT della Banca. In particolare, la Banca registra le informazioni relative sia agli accessi autorizzati, che quelle relative ai tentavi di accesso non autorizzato;
- nell'adozione di sistemi di blocco automatico delle postazioni di lavoro dopo un determinato periodo di tempo di inutilizzo.

All'atto della cessazione del rapporto di lavoro, tutti i "privilegi" per l'accesso ai sistemi informatici vengono revocati

Tutti i dispositivi mobili assegnati ai Collaboratori della Banca (laptop, smartphone, tablet, ecc.) sono dotati di strumenti di autentificazione all'acceso, di criptazione dei dati e, inoltre, consentono il blocco da remoto degli accessi dove necessario, e.g. in caso di furto o smarrimento.

Con riferimento, invece, all'accesso fisico ai Sistemi ICT, la Banca ha previsto misure finalizzate a garantire la sicurezza delle risorse tecnologiche della Banca e prevenire la potenziale manomissione delle stesse.

In particolare, la Banca ha adottato specifici presidi al fine di prevenire accessi non autorizzati ai diversi locali in cui sono collocati gli Strumenti ICT e in particolare i server aziendali (modulati in base alla sensibilità delle risorse tecnologiche), nonché "misure anti-intrusione" volte a garantire un'adeguata sorveglianza degli accessi ai locali della Banca. Tali misure comprendono, a titolo esemplificativo, l'installazione di sistemi di allarme per la rilevazione delle presenze, la predisposizione di centrali di allarme per l'elaborazione dei segnali prodotti dai sistemi di allarme e la registrazione degli eventi segnalati, il collegamento dei sistemi di allarme ad una società di sorveglianza esterna.

e. Gestione dei dati

La Banca tratta e classifica le informazioni in base alla loro criticità e confidenzialità. Con specifico riferimento ai dati relativi ai clienti (c.d. "*Client Identyfing Data*" o "CID"), la Banca classifica tali dati in una delle seguenti categorie in base alla possibilità che gli stessi possano consentire l'identificazione del cliente e adotta tecniche di gestione delle informazioni adeguate a ciascuna classe di informazioni (es. cifratura, anonimizzazione, pseudonimizzazione):

a) dati suscettibili di diretta identificazione: informazioni classificate come "Segrete";
b) dati suscettibili di indiretta identificazione: informazioni classificate come "Confidenziali"";
c) dati potenzialmente suscettibili di indiretta identificazione: informazioni classificate come "Interne".

Al fine di proteggere la confidenzialità e l'integrità delle informazioni, la Banca adotta specifici presidi sia con riferimento ai documenti cartacei (e, più in generale, ai dispositivi fisici di archiviazione, di seguito i "**Dati Fisici**"), che con riferimento ai dati informatici.

Per quanto attiene ai dati e i documenti informatici, è previsto:

a) l'assegnazione di diversi "privilegi" di accesso alle cartelle di rete e ai sistemi gestionali in cui sono custoditi dati e informazioni aziendali;
b) l'obbligo in capo ai Collaboratori di non divulgare le proprie credenziali di accesso e di bloccare lo schermo dei terminali da loro utilizzati quando si allontanano dalla propria postazione (la riattivazione del terminale avviene esclusivamente attraverso l'inserimento delle credenziali assegnate a ciascun Collaboratore);
c) il divieto di esportare e divulgare all'esterno dati e documenti aziendali, salvo che ciò non sia necessario per il regolare svolgimento delle attività aziendali e comunque nel rispetto delle procedure autorizzative aziendali e delle misure di sicurezza adottate;
d) il divieto di trasferire dati conservati nei dispositivi della Banca verso altri sistemi di archiviazione fisica (es. chiavette USB). Le periferiche di connessione di tali terminali sono conseguentemente disabilitate prima che gli stessi siano assegnati ai Collaboratori.

Inoltre, al fine di assicurare un controllo sull'eventuale trasferimento non autorizzato di dati, i dispositivi della Banca sono dotati di appositi applicativi che consentono di individuare eventuali tentativi di manomissione (c.d. "*audit*").

La Banca vieta ai Collaboratori di portare all'esterno del perimetro aziendale gli Strumenti ITC dai medesimi utilizzati, se non per esigenze lavorative.

Per quanto attiene ai Dati Fisici, essi devono essere conservati in cassettiere e armadi chiusi a chiave quando non utilizzati e smaltiti secondo procedure formalizzate.

2.4. Vulnerabilità dovute ad eventi straordinari

Al fine di prevenire che eventi straordinari rispetto alla normale operatività della Banca agevolino la commissione dei reati di cui alla presente Sezione di Parte Speciale, la Banca ha adottato specifici presidi volti a far fronte alle eventuali vulnerabilità che, conseguentemente all'occorrenza di tali eventi straordinari, potrebbero interessare il Sistema ICT.

– *Gestione degli incidenti di sicurezza*

Gli incidenti informatici (disservizi, anomalie sui dati, incidenti riguardanti la sicurezza informatica, ecc.) (di seguito, gli "**Incidenti**") sono gestiti dalla Banca secondo procedure formalizzate al fine di ripristinare tempestivamente le normali condizioni di esercizio degli Strumenti ICT, nonché la qualità e la sicurezza dei dati.

In particolare, al fine di gestire gli Incidenti la Banca provvede a:

- registrare tempestivamente gli Incidenti nel sistema di gestione della Banca, con indicazione del segnalatore ed una descrizione dell'Incidente;
- identificare la tipologia di Incidente;
- valutare il livello di gravità dell'Incidente ed assegnare un livello di "*severity*" da cui dipendono le modalità operative per la gestione dell'Incidente (es: *escalation* funzionale o gerarchica);
- coordinare le attività delle varie unità organizzative per l'analisi dell'Incidente e l'esecuzione delle attività necessarie alla risoluzione dello stesso;
- verificare l'effettiva risoluzione dell'Incidente;
- registrare la positiva gestione dell'Incidente al fine di conservare le informazioni utili alla gestione di incidenti informatici simili.

Ogni Collaboratore della Banca che, nell'ambito della propria attività lavorativa, sia a contatto con le risorse informatiche aziendali è tenuto a segnalare eventuali Incidenti di cui sia a conoscenza.

– *Gestione della continuità operativa*

La Banca ha adottato un piano di continuità operativa (Norma Operativa 11.8 recante "Business Continuity Plan") al fine di garantire, *inter alia*, il ripristino delle componenti del Sistema ICT eventualmente coinvolte in Incidenti che, in considerazione della loro gravità e degli effetti sul sistema informatico della Banca, abbiano determinato una situazione di crisi. In particolare, la Banca in virtù di detto piano ha:

- individuato i soggetti coinvolti nella gestione della continuità operativa della Banca;
- istituito un "Comitato di crisi" presieduto dal COO per la valutazione e la gestione delle situazioni di crisi;

- predisposto una procedura per la gestione delle situazioni di crisi che, in particolare, regola:

  a) la dichiarazione dello stato di crisi;
  b) i flussi informativi;
  c) le contromisure da adottare per i diversi scenari;
  d) le attività di training (simulazione) organizzate in preparazione di eventuali situazioni di crisi.

3. Reati di criminalità organizzata (art. 24-ter del Decreto) e Reati transnazionali (art. 10, L. 16 marzo 2006, n. 146)

3.1. Reati di criminalità organizzata

L'art. 24-*ter* del Decreto prevede come reato presupposto un gruppo di reati inerenti alle varie forme di associazioni criminose, e in particolare:

- associazione per delinquere (art. 416 c.p.);
- associazione di tipo mafioso (art. 416-*bis* c.p.);
- associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del Testo Unico di cui al DPR n. 43/1973);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico di cui al DPR n. 309/1990);

La fattispecie di associazione per delinquere generica (art. 416 c.p.) punisce il semplice fatto di associarsi, in tre o più persone, allo scopo di commettere più delitti (di qualsiasi tipologia). Partecipa all'associazione, peraltro, colui che vi esplichi qualsiasi attività, ancorché secondaria; ed è proprio in tale vincolo associativo, dotato di permanenza o almeno di stabilità - oltre che nel numero minimo di tre associati e nell'indeterminatezza del programma criminoso - che vengono identificati i requisiti caratterizzanti dell'associazione a delinquere e a differenziarla dall'ipotesi del mero concorso nel reato (c.d. "concorso esterno").

La peculiarità dell'associazione di tipo mafioso (art. 416-*bis* c.p.) sta nell'utilizzo del "metodo mafioso", che si realizza "*quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri*".

Assume, inoltre, rilevanza ai fini della responsabilità dell'ente qualsiasi fattispecie delittuosa che comunque venga realizzata avvalendosi del suddetto "*metodo mafioso*": cioè allorquando il soggetto agente, pur senza appartenere al sodalizio criminoso o concorrere con esso, pone in essere una condotta idonea ad esercitare una particolare intimidazione (ad esempio una richiesta nei confronti di una controparte, pubblica o privata) avvalendosi dello sfruttamento della "fama" di organizzazioni criminali operanti nell'ambito di un determinato territorio.

Infine, ai sensi dell'art. 24-*ter* del Decreto rilevano anche tutte le condotte illecite che, sebbene autonomamente non previste quali reati presupposto ai fini dell'applicazione del Decreto, siano poste in essere allo scopo di agevolare l'attività di un'associazione di tipo mafioso (ad esempio il concorso nella commissione di una truffa finanziaria essendo a conoscenza della riferibilità dell'operazione ad una associazione mafiosa).

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

È importante specificare che il reato di associazione a delinquere può essere commesso da chiunque promuova, costituisca o partecipi ad una associazione che ha come scopo quello di commettere più delitti. In particolare, il reato associativo è caratterizzato dai seguenti elementi:

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

Rientrano tra i reati presupposto di criminalità organizzativa ai sensi dell'art. 24-*ter* del Decreto anche le seguenti fattispecie, che non sono state considerate rilevanti con riferimento all'operatività della Banca:

- scambio elettorale politico mafioso (416 ter c.p.), ossia l'ottenimento della promessa di voti per sé o ad altri in occasione di consultazioni elettorali in cambio dell'erogazione di denaro;
- sequestro di persona a scopo di rapina o di estorsione (630 c.p.);
- illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407 c.p.p.).

3.2. Reati transnazionali

L'art. 3 della L. 16 marzo 2006, n. 146 ("Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001", di seguito "**L. 146/2006**") ha introdotto nella normativa penale italiana la nuova categoria dei "reati transnazionali".

All'art. 10 della L. 146/2006 è prevista l'estensione della disciplina del Decreto in riferimento ad alcuni reati, ove ricorrano le condizioni di cui all'art. 3 perché il reato possa considerarsi "transnazionale". Ai sensi dell'art. 3 della L. 146/2006, 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, alternativamente:

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

Per "gruppo criminale organizzato", ai sensi della Convenzione, si intende "*un gruppo strutturato, esistente per un periodo di tempo, composto da tre o più persone che agiscono di concerto al fine di commettere uno o più reati gravi o reati stabiliti dalla convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale*".

L'art. 10 della stessa L. 146/2006 ha esteso la punibilità degli enti ai sensi del Decreto anche ai "*reati transnazionali*", sebbene limitandola ad un elenco specifico di fattispecie, ed in particolare ai seguenti reati:

- reati associativi e, in particolare, i reati di:
  - associazione per delinquere (art. 416 c.p.);
  - associazione di tipo mafioso (art. 416-*bis* c.p.);
  - associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-*quater* del Testo Unico di cui al DPR n. 43/1973);
  - associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico di cui al DPR n. 309/1990);
- reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.);
- reato di favoreggiamento personale (art. 378 c.p.);
- reati concernenti il traffico di immigrati (ossia, disposizioni contro le immigrazioni clandestine, art. 12 D.Lgs. 286/1998).

I reati associativi sopra indicati e il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria sono già previsti quali autonomi reati presupposto della responsabilità degli enti - cioè, anche se commessi in una dimensione meramente nazionale – rispettivamente ai sensi degli artt. 24-*ter* del Decreto (trattati nella presente Sezione della Parte Speciale del Modello) e 25-*decies* del Decreto (cfr. Sezione 1 della presente Parte Speciale del Modello). Con riferimento a queste fattispecie, il carattere "transnazionale" non assume una funzione estensiva della responsabilità della persona giuridica ai sensi del Decreto, incidendo esclusivamente sulla comminatoria edittale di pena per il fatto commesso.

Il reato, invece, di favoreggiamento personale (art. 378 c.p.) assume rilevanza ai fini del Decreto soltanto qualora qualificabile come "reato transnazionale". Tale reato consiste nel prestare aiuto a taluno - dopo l'avvenuta commissione di un delitto per il quale la legge stabilisce l'ergastolo o la reclusione e fuori dei casi di concorso nel medesimo - ad eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa. Il reato sussiste anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto. Si precisa che, per giurisprudenza maggioritaria, integrano il reato anche le false risposte, rese ai fini di cui sopra, alle richieste dell'autorità giudiziaria.

Con riferimento ai reati concernenti il traffico di immigrati, considerata la natura dell'attività svolta dalla Banca, si è escluso il rischio di commissione di tali reati nel contesto aziendale.

3.3. Attività aziendali sensibili

Nell'ambito dell'attività della Banca il rischio che siano posti in essere i reati associativi sopra indicati è legato soprattutto al rischio di mettere a disposizione della clientela (soprattutto ove appartenente o comunque contigua alla malavita organizzata), servizi bancari, servizi o risorse finanziarie che risultino strumentali al perseguimento di attività illecite.

La Banca potrebbe essere esposta al rischio di commissione di reati di criminalità organizzata nello svolgimento delle seguenti attività: (i) selezione del personale, in relazione alla possibilità che tale attività sia strumentalizzata per infiltrare nell'organizzazione della Banca persone coinvolte in associazioni per delinquere o mafiose, con il conseguente rischio di asservire la Banca alla realizzazione degli scopi dell'associazione per delinquere o mafiosa; (ii) instaurazione di rapporti

contrattuali con soggetti, persone fisiche o giuridiche, coinvolte in associazioni criminali o che abbiano precedenti penali per partecipazione o concorso in associazione per delinquere o mafiosa.

Per quanto concerne il rischio di commissione del reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.) si rinvia a quanto indicato nella Sezione 1 della Parte Speciale del presente Modello relativa ai reati contro la Pubblica Amministrazione.

Con riferimento, invece, al reato di favoreggiamento personale (ove rilevante come reato transnazionale), la Banca potrebbe essere esposta al rischio di commissione di tale reato ove la Banca o un Destinatario riceva richieste da parte di un'autorità giudiziaria. Con riguardo alla fattispecie delittuosa in esame, il rischio di commissione del reato è potenzialmente presente in tutte le unità organizzative.

La Banca ha dunque individuato le seguenti attività aziendali sensibili:

a) instaurazione e gestione dei rapporti con la clientela;
b) attività di selezione del personale;
c) instaurazione di rapporti contrattuali;
d) rapporti con le autorità giudiziarie.

Con riguardo alle fattispecie delittuose e attività aziendali sensibili sopra individuate le unità organizzative della Banca principalmente coinvolte sono:

- Funzione L&C;
- Risorse Umane;
- Funzioni Proponenti e Funzioni Referenti nell'ambito dei processi di selezione dei fornitori;
- Front Office;
- gli organi e le funzioni aziendali aventi ruoli e responsabilità nel sistema di governance e di controlli interni in materia di lotta contro il riciclaggio e il finanziamento del terrorismo. (cfr. Sezione 7 della Parte Speciale del presente Modello).

3.4. Principi di controllo e di comportamento e protocollo aziendale

Si riportano di seguito i presidi che la Banca adotta in relazione alle diverse attività aziendali sensibili al fine di prevenire la commissione dei reati oggetto della presente Sezione di Parte Speciale

3.4.1. Instaurazione e gestione dei rapporti con la clientela

Le attività aziendali sensibili rilevanti ai fini dei reati in oggetto coincidono con quelle in cui è più alto il rischio che si verifichino anche reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita. Il sistema di controlli, nonché le policy e le procedure interne già individuate con riferimento a tali reati trovano, pertanto, applicazione anche in relazione alla prevenzione dei reati oggetto della presente Sezione di Parte Speciale.

Tali presidi sono basati principalmente sul rispetto delle procedure volte all'acquisizione di un'approfondita conoscenza della clientela, delle controparti e delle relative operazioni, sia in sede di c.d. *onboarding* sia in via continuativa (cfr. Sezione 7 della Parte Speciale del presente Modello).

3.4.2. Selezione del personale

Per quanto riguarda l'attività di gestione del personale la Banca ha adottato la Norma Operativa 4.15 "*Assunzione di Personale"* volta a definire i presupposti, le attività e le responsabilità della ricerca, selezione ed assunzione di Collaboratori.

Sono ritenuti idonei al fine di prevenire i reati oggetto della presente Sezione di Parte Speciale i presìdi previsti in tema prevenzione dei reati contro la pubblica amministrazione nell'ambito del processo di assunzione del personale già descritti nella Sezione 1 della Parte Speciale del presente Modello.

3.4.3. Instaurazione di rapporti contrattuali

I presìdi adottati per la prevenzione dei reati associativi in connessione con l'instaurazione di rapporti contrattuali con controparti terze (fornitori e professionisti esterni) coincidono con i presidi adottati al fine di prevenire i reati di corruzione. Nell'ambito dell'attività di selezione dei fornitori e conferimento degli incarichi professionali la Banca ha adottato una specifica norma operativa (Norma Operativa n. 12.2. "*Norma Operativa in materia di procurement"*), che disciplina le modalità di selezione, contrattualizzazione nonché supervisione dei fornitori e degli *outsourcer* e i cui contenuti sono descritti nella Sezione 1 della Parte Speciale del presente Modello.

3.4.4. Rapporti con le autorità giudiziarie

In generale, è previsto un divieto in capo ad ogni Destinatario di emettere dichiarazioni o rilasciare a qualsiasi pubblica amministrazione, inclusa qualsiasi autorità giudiziaria, dati, documenti o informazioni non corrispondenti al vero nonché di richiedere o indurre testimoni di un procedimento penale di tenere comportamenti reticenti o mendaci a favore della Banca.

Si richiamano, inoltre, gli ulteriori presidi in materia di gestione dei procedimenti pendenti davanti alle autorità giudiziarie adottati dalla Banca con la Norma Operativa 5.60 per la gestione di "*Decreti / Ordinanze dell'autorità giudiziaria, lettere di risposta all'autorità*" e descritti nella Sezione 1 della Parte Speciale del presente Modello).

4. Delitti contro l'industria e il commercio (art. 25-bis.1)

4.1. Fattispecie delittuose

4.1.1. Frode nell'esercizio del commercio

Ai sensi dell'art. 515 c.p., commette reato chiunque, nell'esercizio di una attività commerciale, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita. La norma trova applicazione solo ove il fatto non costituisca più grave reato.

Ai fini della configurazione del reato in oggetto, si precisa che per "bene mobile" si intende qualsiasi bene materiale, ad esclusione del denaro.

Tale condotta potrebbe realizzarsi nel caso in cui, ad esempio, la Banca, per il tramite di un Collaboratore, contribuisca alla commissione del reato in esame da parte di un proprio cliente in Italia con l'attribuzione allo stesso di beni in oro di qualità differente da quella dichiarata.

4.1.2. Attività aziendali sensibili

Il rischio di commissione di condotte che integrino la fattispecie di reato in oggetto può presentarsi nell'ambito dei rapporti con la clientela, con riguardo alle seguenti attività:

- accettazione e consegna di averi fisici (ad esempio, metalli preziosi e altri beni preziosi affidati in custodia alla Banca).

Con riguardo alla fattispecie delittuosa sopra individuata, le Unità organizzative principalmente coinvolte sono:

- Funzione Legal & Compliance;
- Ufficio Formalità Clientela;
- Ufficio Cassa;
- Ufficio Titoli.

4.1.3. Principi di controllo e di comportamento e protocollo aziendale

Come già precisato nella sezione 7 della Parte Speciale del Modello, relativa ai "*reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e autoriciclaggio (art. 25-octies) e reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater)*", l'attività di custodia di valori fisici e di locazione di cassette di sicurezza è svolta dalla Banca in misura marginale rispetto al business aziendale e comunque su specifica richiesta da parte dei clienti.

Ciò premesso, tutti i Collaboratori sono obbligati ad astenersi da qualsiasi condotta che possa costituire una fattispecie di frode nell'esercizio del commercio e sono tenuti a segnalare ogni condotta illecita di cui vengano a conoscenza tramite i canali di segnalazione previsti dal presente Modello (cfr. Sezione 2.11 della Parte Generale del presente Modello).

La Banca ha, inoltre, adottato specifiche Norme Operative (Cfr. Norma Operativa 5.52 "*Valori fisici in custodia presso PKB*" e Norma Operativa 5.12 "*cassette di sicurezza*") che disciplinano i presidi adottati in relazione alla gestione di averi fisici depositati dai clienti presso la Banca, nell'ambito delle seguenti forme di custodia e deposito:

1. custodia individuale di beni personali dei clienti in cassette di sicurezza individuali (c.d. locazione di cassette di sicurezza);

2. deposito di valori fisici di proprietà del cliente in custodia presso il tesoro della Banca (c.d. "*custodia individuale*");
3. custodia di metalli preziosi dei clienti in un deposito collettivo, eventualmente assieme alle consistenze della Banca (c.d. "*custodia globale*").

Con specifico riferimento agli averi fisici depositati dalla clientela in cassette di sicurezza, si precisa – ai fini dell'ipotetica configurazione dei reati oggetto della presente Parte Speciale - che la Banca, come previsto dalla normativa svizzera applicabile, non viene a conoscenza dei beni ivi depositati dal cliente, salvo che siano notificati ordini di sequestro da parte della Procura Pubblica svizzera.

La Norma Operativa 5.12 "*cassette di sicurezza*" disciplina il processo di affidamento in locazione delle cassette di sicurezza e di utilizzo delle stesse da parte dei clienti, prevedendo misure che garantiscono la massima riservatezza dei beni depositati.

Con riferimento alla custodia individuale di valori fisici dei clienti, in custodia presso il tesoro della Banca, è stata adottata la Norma Operativa 5.52 "*Valori Fisici in custodia presso PKB*", che prevede:

- la definizione di ruoli e responsabilità delle unità organizzative e degli uffici competenti in relazione al deposito presso la Banca stessa delle diverse tipologie di beni depositabili;
- per ciascuna tipologia di beni depositati, la disciplina delle attività che i Collaboratori della Banca sono tenuti a porre in essere in caso di primo deposito, movimentazione o prelievo dei beni depositati (a titolo esemplificativo, imballaggi, registrazioni, verifiche della documentazione, consegna della ricevuta al cliente, riconciliazione dei conti ecc.);
- la registrazione dei beni depositati presso la Banca in apposito sistema informatico;
- la consegna al cliente dei valori avviene solo previa verifica dell'identità del cliente e dell'originalità della firma apposta sulla ricevuta per il ritiro;
- un controllo almeno annuale, a cura dell'ufficio competente, sui beni depositati nel Tesoro, verificandone la corrispondenza alla lista dei beni registrati nel sistema informatico;
- controlli a campione su base trimestrale da parte dei responsabili degli uffici competenti;
- conservazione della documentazione relativa agli inventari effettuati per almeno 3 anni.

Si precisa che la Banca presta il servizio di deposito solo su espressa richiesta del cliente e comunque, in via del tutto eccezionale.

5. Reati societari (art. 25-ter)

5.1. Premessa

Nella presente sezione sono state considerate alcune fattispecie di reato relative ai c.d. reati societari (art. 25-ter del Decreto) di potenziale rilevanza per la Banca. Considerato che la Banca è una società regolata dal diritto svizzero, le fattispecie di reato considerate nella presente Sezione di Parte Speciale potrebbero, assumere rilevanza per la Banca medesima in relazione a:

1. la gestione di partecipazioni sociali in società di diritto italiano, che alla data di adozione del presente Modello risultano essere le seguenti:
   - Cassa Lombarda S.p.A., (partecipazione diretta pari al 99,57% del capitale sociale;
   - PKB Servizi Fiduciari S.p.A. (partecipazione diretta pari al 70% del capitale sociale);
   - Anthilia Capital Partner SGR S.p.A. (partecipazione diretta pari al 10,60% del capitale sociale);
   - Fenera & Partners SGR S.p.A. (partecipazione diretta pari al 2,5% del capitale sociale)

   La Banca detiene, inoltre, partecipazioni indirette tramite Cassa Lombarda S.p.A., in PKB Servizi Fiduciari S.p.A. (30% del capitale sociale), Anthilia Capital Partner SGR S.p.A. (9,15% del capitale sociale), SIA SpA (0,00376%) e SWIFT (0,0027%).
2. il concorso dei Dipendenti nella commissione di reati societari con clienti rientranti nella categoria di clientela c.d. corporate (ad es, mediante istigazione ovvero produzione di documentazione bancaria contraffatta o falsa).

I reati presupposto di corruzione tra privati e di istigazione alla corruzione tra privati di cui agli artt. 2635, co. 3, e 2635-bis c.c. (rilevante ai sensi dell'art. 25-ter del Decreto), sono stati considerati nella Sezione 1 della Parte Speciale del Modello.

Per il reato di aggiotaggio ai sensi dell'art. 2637 c.c. (rilevante ai sensi dell'art. 25-ter del Decreto) si rinvia, invece, alla Sezione 6 della Parte Speciale del Modello.

5.2. Fattispecie di reato

5.2.1. False comunicazioni sociali (relative a società non quotate)

La fattispecie di reato in oggetto è disciplinata dall'art. 2621 c.c. e si configura nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società non quotate, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente pongono in essere una delle seguenti condotte, in modo concretamente idoneo ad indurre altri in errore:

- espongono fatti materiali rilevanti non rispondenti al vero; ovvero
- omettono fatti materiali rilevanti, la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene.

L'illecito sussiste anche se la condotta si riferisce a beni posseduti o amministrati dalla società per conto terzi. Se i fatti di cui all'articolo 2621 c.c. sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta**,** si applica una sanzione ridotta.

5.2.2. Impedito controllo

L'art. 2625 c.c. punisce la condotta degli amministratori che occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali sempre che la condotta abbia cagionato un danno ai soci.

5.2.3. Indebita restituzione di conferimenti

L'art. 2626 c.c. punisce la condotta degli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

5.2.4. Illegale ripartizione degli utili e delle riserve

Salvo che il fatto non costituisca più grave reato, l'art. 2627 c.c. punisce la condotta degli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite.

5.2.5. Illecite operazioni sulle azioni o quote sociali o della società controllante

L'art. 2628 c.c. punisce la condotta degli amministratori che, fuori dei casi consentiti dalla legge:

- acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge ovvero,
- acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

5.2.6. Operazioni in pregiudizio dei creditori

L'art. 2629 c.c. punisce la condotta degli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale, fusioni con altre società o scissioni, cagionando danno ai creditori.

5.2.7. Formazione fittizia del capitale

L'art. 2632 c.c. punisce la condotta degli amministratori che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante:

- attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

5.2.8. Indebita ripartizione dei beni sociali da parte dei liquidatori

L'art 2633 del c.c. sanziona la condotta degli eventuali liquidatori della società che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori.

Il reato in oggetto è punibile a querela della persona offesa e il risarcimento del danno ai creditori prima del giudizio estingue il reato.

5.2.9. Illecita influenza sull'assemblea

L'art. 2636 del c.c. punisce chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

5.2.10. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

L'art. 2638 c.c. sanziona la condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori di soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza:

- Espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza (anche nel caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi); ovvero
- occultano con altri mezzi fraudolenti, in tutto o in parte, fatti che avrebbero dovuto comunicare, concernenti la situazione medesima (anche nel caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi);
- in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

5.3. Attività aziendali sensibili

La Banca ha identificato le seguenti attività aziendali sensibili, per le quali è maggiore il rischio che siano posti in essere i reati oggetto della presente Sezione di Parte speciale, ove interessino rapporti tra la Banca e la clientela italiana *corporate*, oppure siano inerenti a partecipazioni in società di diritto italiano detenute dalla Banca:

a) gestione dei rapporti con la clientela e produzione di reportistica periodica;
b) gestione delle partecipazioni sociali;
c) gestione dei rapporti con le Autorità di Vigilanza;
d) reportistica fiscale alla clientela.

Con riguardo alle fattispecie delittuose sopra individuate, le Unità organizzative principalmente coinvolte sono:

- Consiglio di Amministrazione
- Direzione Generale;
- Risk Management;
- Contabilità;
- Legal & Compliance;
- Corporate Banking.
- Relationship Manager;
- Funzione ICT;
- Ufficio Formalità Clientela;

Per i principi e i presìdi in materia di gestione dei rapporti con le Autorità di Vigilanza si rinvia a quanto previsto con riferimento alla prevenzione dei reati commessi nei rapporti con la Pubblica Amministrazione (Sezione 1 della Parte Speciale del Modello).

Con riferimento, invece, alla reportistica fiscale, si rinvia ai presidi e ai principi previsti dalla Parte Speciale relativa ai Reati tributari (Sezione 8 della Parte Speciale del Modello).

5.4. Principi di controllo e di comportamento e protocollo aziendale

a. Gestione dei rapporti con la clientela, produzione di reportistica periodica

Con riferimento al rischio di concorso della Banca nella commissione di reati societari con i clienti *corporate*, al personale della Banca stessa, impiegato nella gestione dei rapporti con la clientela, è fatto divieto di:

- rappresentare o trasmettere ai clienti *corporate* dati bancari, riguardanti la relativa situazione patrimoniale e finanziaria falsi, fuorvianti o, comunque, non rispondenti alla realtà;
- omettere dati ed informazioni riguardanti la situazione patrimoniale e finanziaria dei clienti.

Al fine di prevenire il coinvolgimento della Banca nei reati oggetto della presente Sezione di Parte Speciale, la Banca ha adottato un processo di produzione documentale automatizzato ed idoneo a garantire l'immodificabilità della documentazione relativa alla situazione patrimoniale e finanziaria del cliente. In particolare:

- tutte le operazioni compiute dai clienti sulle relative relazioni bancarie sono registrate, conservate e archiviate per un periodo di 10 anni, in formato immodificabile nel sistema informatico adottato dalla Banca;
- tutte le operazioni registrate nel sistema informatico della Banca non automatizzate sono soggette a procedure autorizzative basate sul principio del "4 eyes" nonché a specifiche verifiche sulla correttezza dei dati imputati;
- i documenti relativi alla situazione patrimoniale e finanziaria dei clienti (ad esempio, estratti conto, rendiconti annuali etc.) sono prodotti attraverso procedure informatiche, automatiche e interamente tracciabili, che estraggono dati e informazioni direttamente dal sistema informatico in uso;
- i documenti relativi alla situazione patrimoniale e finanziaria dei clienti sono prodotti in formati standard, generati automaticamente dal sistema informatico aziendale, anche nel caso in cui i medesimi siano trasmessi *brevi manu* al cliente nel corso di riunioni fisiche;
- i documenti relativi alle relazioni bancarie aperte dalla clientela presso la Banca, quando pubblicati sull'*e-banking* dei clienti, sono prodotti in formato non modificabile;
- Le procedure di rettifica dei dati prevedono processi di escalation che coinvolgono diversi livelli organizzativi e garantiscono la tracciabilità delle modifiche apportate. In particolare, il cliente viene informato, tramite specifica comunicazione, in merito alla correzione di dati e informazioni che sono risultati errati;
- tutti i dati, le informazioni e i documenti raccolti per ciascun cliente sono conservati e registrati nel sistema informatico specificamente adottato a tal fine;

L'apertura di conti correnti a servizio del deposito del capitale sociale da parte di società straniere è sottoposta al preventivo rilascio di un'attestazione da parte di un notaio o avvocato di tale giurisdizione che attesti la legittimità di tale deposito presso istituti bancari stranieri (i.e. svizzeri). In tali casi, la Banca applica la Norma Operativa 2.47 "*Apertura conti per la costituzione di società (versamento capitale sociale) o richieste di aumento del capitale di società esistenti*".

b. Gestione delle partecipazioni sociali

La Banca ha adottato regole di comportamento al fine di garantire una gestione corretta a trasparente delle partecipazioni societarie dalla medesima detenute, evitando di porre in essere condotte che possano determinare la commissione di reati societari o il concorso della Banca con amministratori, direttori, liquidatori e dirigenti delle società partecipate, nella commissione di reati societari di cui alla presente Sezione di Parte Speciale.

In particolare, al personale coinvolto nella gestione della partecipazione sociale è fatto divieto di porre in essere le seguenti condotte:

- porre in essere comportamenti che impediscano, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che in qualsiasi altro modo ostacolino lo svolgimento dell'attività di controllo e di revisione da parte degli organi societari o l'esercizio delle funzioni di vigilanza da parte delle autorità italiane;
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, le comunicazioni di dati, informazioni e documenti previste dalle disposizioni normative e regolamentari applicabili e/o richieste dalle Autorità di Vigilanza in relazione alla qualità di socio che la Banca ricopre nelle società partecipate;
- determinare la maggioranza o influenzare l'assunzione di deliberazioni in assemblea con atti simulati o fraudolenti con lo scopo di procurare a sé o ad altri un ingiusto profitto;
- determinare gli amministratori della società partecipata alla restituzione illecita dei conferimenti;
- violare le disposizioni normative relative alla tutela dell'integrità ed effettività del patrimonio sociale, poste a garanzia dei creditori e dei terzi in genere;
- deliberare in merito a riduzioni del capitale sociale, fusioni o scissioni delle società controllate in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- deliberare in merito ad aumenti fittizi del capitale sociale delle società controllate, attribuendo azioni per un valore inferiore al loro valore nominale.

Con specifico riferimento alla trasmissione di informazioni alle Autorità di Vigilanza, tra cui le autorità di vigilanza italiane, oltre ai presidi di cui alla Sezione 1.3. della presente Parte Speciale relativi ai rapporti con la pubblica amministrazione, la Banca:

- provvede a trasmettere i dati contabili rilevanti a Cassa Lombarda (individuata da Banca d'Italia come soggetto referente delle segnalazioni di vigilanza consolidata del Gruppo PKB) tramite un sistema informatico che consolida i dati del Gruppo bancario;
- ha adottato sistemi informatici che consentono di elaborare in modo semi-automatico la reportistica periodica richiesta dalle Autorità di Vigilanza, estraendo dati e informazioni dal "*Core Banking System*" e adeguandoli, con le necessarie rettifiche, ai principi contabili IFRS;
- pone in essere controlli di primo e secondo livello sulla reportistica richiesta dall'Autorità di Vigilanza italiana in relazione alle partecipazioni detenute in società italiane soggette a vigilanza;

Con specifico riferimento al sistema informatico "Core Banking System" da cui originano i dati oggetto delle segnalazioni alle Autorità di Vigilanza, si rileva quanto segue:

- il Core Banking System è un sistema informatico integrato che raccoglie e registra tutti i dati relativi alle operazioni effettuate dalla Banca (inclusi i dati imputati nel sistema di ciclo passivo) e dai clienti;

- il Core Banking System genera automaticamente i dati contabili della Banca, garantendo la costante riconciliazione dei dati relativi alle operazioni bancarie con quelli contabili;
- la Banca ha inoltre adottato un sistema gestionale per l'interrogazione e l'estrazione dal Core Banking System delle informazioni rilevanti ai fini della produzione delle segnalazioni di vigilanza;
- i dati registrati nel Core Banking System non sono modificabili, salvo la possibilità di effettuare operazioni di rettifica nel rispetto di specifiche procedure interne. Tali operazioni di rettifica sono tracciate e sottoposte a controlli di primo e secondo livello;
- anche al fine di prevenire operazioni fraudolente, è previsto uno stretto monitoraggio delle perdite operative, le quali devono essere tutte supportate da idonei giustificativi e sottoposte a controlli di primo e secondo livello;
- i dati registrati nel Core Banking System e i dati contabili sono soggetti a controlli di secondo e terzo livello, oltre che alla revisione dei conti da parte del revisore esterno che certifica i bilanci della Banca.

Con specifico riferimento alla partecipazione alle assemblee delle società italiane partecipate dalla Banca, sono adottati i seguenti presidi:

- la partecipazione alle assemblee dei soci delle società partecipate, in rappresentanza della Banca, è consentita esclusivamente a soggetti dotati di procura speciale;
- le procure speciali a partecipare alle assemblee delle società partecipate sono rilasciate in forma scritta in relazione, sia ad assemblee ordinarie, sia ad assemblee straordinarie secondo le seguenti modalità:
    - la procura è conferita per una sola assemblea, in prima e seconda convocazione;
    - la procura attribuisce poteri circoscritti agli argomenti posti all'ordine del giorno della riunione alla quale il procuratore partecipa;
- le procure per la partecipazione alle assemblee delle società partecipate e le relative istruzioni di voto sono rilasciate da 2 membri della Direzione Generale a seguito di specifica analisi dell'ordine del giorno dell'assemblea stessa e della documentazione allegata.

6. Reati ed illeciti amministrativi riconducibili ad "abusi di mercato" (art. 25-sexies)

6.1. Premessa

L'art. 25-sexies del Decreto include tra i reati presupposto anche le fattispecie di reato di abuso di informazioni privilegiate e di manipolazione del mercato previste ai sensi degli artt. 184 e 185 del decreto legislativo 24 febbraio 1998, n. 58 ("**TUF**").

L'ambito della condotta vietata è delineato dagli articoli del TUF richiamati in conformità con le previsioni del Regolamento (UE) n. 596/2014 (Market Abuse Regulation - "**MAR**") e della Direttiva 2014/57/UE (Market Abuse Directive II - "**MAD II**").

In particolare, la MAR ha introdotto un quadro normativo uniforme nell'Unione Europea in materia di abusi di mercato, in sostituzione della disciplina precedentemente prevista da ciascun ordinamento degli Stati Membri in attuazione della abrogata direttiva 2003/6/CE.

Oltre alle fattispecie di reato richiamate espressamente dall'art. 25-sexies del Decreto, il TUF prevede delle fattispecie di illecito amministrativo ai sensi degli artt. 187-bis e 187-ter del TUF, rispettivamente per il caso di abuso e comunicazione illecita di informazioni privilegiate in violazione dell'art. 14 MAR nonché per il caso di manipolazione del mercato ai sensi dell'art. 15 MAR.

Lo stesso TUF (art. 187-*quinquies*), poi, prevede una potenziale responsabilità amministrativa per gli enti, in aggiunta a quella prevista dal Decreto, per il caso in cui sia commessa nel suo interesse o a suo vantaggio una violazione del divieto di cui all'articolo 14 MAR o del divieto di cui all'articolo 15 del MAR, con regole di imputabilità per l'Ente analoghe a quelle del D. Lgs. n. 231/2001.

L' 187 *ter*.1 TUF, inoltre, introdotto dal D. lgs. 10 agosto 2018, n. 107, prevede sanzioni amministrative a carico di ciascun ente o società per la violazione di disposizioni specifiche contenute nel MAR.

Salvo quanto meglio si specificherà con riferimento a ciascuno dei diversi illeciti, le condotte punite possono avere per oggetto:

a) strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altri Paesi dell'Unione europea;
b) strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata richiesta di ammissione alle negoziazioni in un sistema multilaterale di negoziazione (c.d. MTF) italiano o di altri Paesi UE;
c) strumenti finanziari negoziati su un sistema organizzato di negoziazione (c.d. OTF) italiano o di altro Paese UE;
d) altri strumenti finanziari non contemplati nelle precedenti lettere, il cui prezzo o valore di strumenti negoziati nelle sedi di cui alle precedenti lettere o ha effetto sugli stessi, compresi i credit default swap e i contratti differenziali;
e) condotte o alle operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari, ai sensi del regolamento (UE) n. 1031/2010.

Con riferimento all'ambito di applicazione territoriale di tali norme, l'art. 182 del TUF precisa che i reati e gli illeciti amministrativi in materia di abusi di mercato sono puniti secondo la legge italiana

sia se commessi in Italia, sia se commessi all'estero, qualora attengano a strumenti finanziari ammessi o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o in un sistema multilaterale di negoziazione italiano (MTF), o a strumenti finanziari negoziati su un sistema organizzato di negoziazione italiano (OTF).

Rientra, infine, tra i reati riconducibili alla materia degli abusi di mercato che possono dar luogo alla responsabilità degli Enti ai sensi dell'art. 25-ter del D.lgs. 231/2001, anche il reato di aggiotaggio (art. 2637 c.c.) con riferimento agli strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato.

Si fornisce di seguito una descrizione dettagliata delle fattispecie di illeciti, riconducibili alla materia degli abusi di mercato, che possono dar luogo alla responsabilità della Banca ai sensi del Decreto.

6.2. Fattispecie delittuose di abuso di mercato

6.2.1. Abuso di informazioni privilegiate (art. 184 TUF)

La fattispecie penale si realizza quando un soggetto, essendo in possesso di informazioni privilegiate in ragione (i) della sua qualità di membro degli organi di amministrazione, direzione o controllo dell'emittente ovvero (ii) della partecipazione al capitale dell'emittente ovvero (iii) dell'esercizio di un'attività lavorativa, professionale ovvero di una funzione o di un ufficio:

a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime (*insider trading*);
b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato (comunicazione illecita di informazioni privilegiate o *tipping*)
c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a) (raccomandazioni o *tuyautage*).

Il reato di cui all'art. 184 TUF può, inoltre, essere commesso da chi sia entrato in possesso di informazioni privilegiate in conseguenza della preparazione o commissione di un reato (es. intrusione in un sistema informatico ed estrazione di informazioni privilegiate).

L'abuso di informazioni privilegiate può essere commesso anche da chiunque, per ragioni diverse da quelle indicate sopra (ossia, al di fuori della carica di membro degli organi di amministrazione direzione e controllo dell'emittente, della partecipazione al capitale sociale dell'emittente, dell'esercizio dell'attività lavorativa, della professione, della funzione o dell'ufficio nonché della preparazione o commissione del reato), conoscendo il carattere privilegiato dell'informazione compie una delle azioni di cui alle lett. a), b) e c) sopra (c.d. "*insider secondario*").

Per informazione privilegiata, ai sensi dell'art. 7, comma 1, del MAR si intende "*un'informazione avente un carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari, e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati*".

Un'informazione si ritiene di carattere preciso se:

- fa riferimento a una serie di circostanze o a un evento verificatisi o che si può ragionevolmente ritenere che vengano a prodursi e

- se tale informazione è sufficientemente specifica da permettere di trarre conclusioni sul possibile effetto sui prezzi degli strumenti finanziari o del relativo strumento finanziario derivato, dei contratti a pronti su merci collegati o dei prodotti oggetto d'asta sulla base delle quote di emissione.

Per informazione che, se comunicata al pubblico, avrebbe probabilmente un effetto significativo sui prezzi s'intende un'informazione che un investitore ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni di investimento.

Nel caso delle persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, per informazione privilegiata si intende anche l'informazione trasmessa da un cliente e concernente gli ordini del cliente in attesa di esecuzione, che ha un carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari

6.2.2. Manipolazione del mercato (art. 185 TUF)

La fattispecie penale si realizza quando qualcuno diffonde notizie false (*information based manipulation*) o pone in essere operazioni simulate o altri artifizi (*action based manipulation*) concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari ([5]).

Non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'art. 13 del MAR.

6.3. Illeciti amministrativi di abuso di mercato (art. 187 bis, art. 187 ter e art. 187 ter.1 TUF)

Gli illeciti amministrativi di cui agli artt. 187 *bis* e 187 *ter* del TUF prevedono fattispecie speculari a quelle contemplate come figure di reato dagli artt. 184 e 185, disponendo l'applicazione di sanzioni amministrative in capo alla persona fisica che agisce, oltre che all'ente (nel caso in cui la violazione sia commessa nel suo interesse o a suo vantaggio), che violi il divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate e il divieto di manipolazione del mercato di cui agli articoli 14 e 15 del MAR.

Il rinvio diretto a tali articoli comprende tutti gli elementi a loro volta implicitamente richiamati dalle due fattispecie disciplinate dal MAR. Ciò implica che la condotta rilevante ai fini dell'applicazione della sanzione amministrativa risulta più ampia di quella rilevante ai fini penali, quest'ultima circoscritta agli elementi espressamente descritti dal TUF per i quali non opera un generale rinvio al MAR .

In particolare, mentre per la configurazione di un illecito penale è necessaria l'esistenza del dolo, per l'illecito amministrativo è sufficiente la colpa.

Ciò non esclude che le medesime condotte possano essere rilevanti ai fini sia penali e sia amministrativi, potendo dare origine ad un cumulo di sanzioni.

[5] L'art. 12 MAR e l'allegato I al MAR definiscono un elenco non tassativo di indicatori connessi all'utilizzo di artifici o di qualsiasi altra forma di inganno o espediente e un elenco non tassativo di indicatori connessi a segnali falsi o fuorvianti e alla fissazione dei prezzi.

6.4. Aggiotaggio (art. 2637 c.c.)

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Secondo l'art. 6 del codice penale, un reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero se si è ivi verificato l'evento che è la conseguenza dell'azione od omissione.

Le norme contenute nell'art. 2637 c.c. non trovano concreta applicazione con riferimento alla Banca in ragione della sua operatività, tenuto anche conto che la Banca non opera su, né diffonde notizie riguardanti, strumenti finanziari italiani non ammessi alla negoziazione su mercati regolamentati, MTF o OTF.

6.5. Attività aziendali sensibili

Le attività "sensibili" della Banca identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati e gli illeciti amministrativi riconducibili ad abusi di mercato sono le seguenti:

- gestione delle informazioni privilegiate;
- gestione degli ordini e delle operazioni di mercato, sia in conto proprio sia per conto della propria clientela.

Con riguardo alle fattispecie delittuose sopra individuate, le Unità organizzative principalmente coinvolte sono:

- Membri del Consiglio di Amministrazione e della CDG;
- Capital Market;
- Consulenti alla clientela;
- Assistenti alla clientela;
- Asset Management (nell'ambito dell'attività sia di c.d. gestione patrimoniale sia di Investor Manager di organismi di investimento collettivo del risparmio);
- Legal & Compliance.

Dall'attività di *risk assessment* svolta dalla Banca è risultato che nel complesso l'operatività della Banca non espone sensibilmente i Collaboratori all'ottenimento d'informazioni privilegiate, non essendo svolte attività di "Investment Banking", "*Merger & Acquisition*" aventi ad oggetto emittenti, o consulenza "Corporate" ed avendo la Banca una ridotta attività di negoziazione per conto proprio.

Tuttavia, informazioni privilegiate potrebbero essere comunque acquisite dai Collaboratori nell'ambito dei rapporti intrattenuti con la propria clientela, soprattutto nei rapporti coi singoli clienti che hanno un legame con società emittenti o che potrebbero comunque essere in possesso di informazioni privilegiate, ovvero in relazione ad operazioni svolte dai clienti che possano avere un impatto sull'andamento delle negoziazioni (in relazione, in particolare, al rischio di c.d. *front* e *parallel running*).

6.6. Principi di controllo e di comportamento e protocollo aziendale

La Banca ha adottato una specifica norma operativa (NO 5.83 Regole di condotta sul mercato) in conformità con la normativa svizzera in materia di abusi di mercato (la "**Norma Operativa Market Abuse**").

La Norma Operativa adottata dalla Banca trova applicazione, oltre che con riferimento agli strumenti finanziari ammessi alla negoziazione sulle *trading venues* svizzere, con riferimento agli strumenti finanziari negoziati su mercati regolamentati, MTF e OTF italiani (e comunque dell'Unione Europea).

La Banca ha adottato, inoltre, una Norma Operativa che impone limitazioni massime all'operatività giornaliera degli operatori sui mercati, sia nell'attività svolta per conto della Banca sia nell'attività svolta per la clientela (cfr. NO 8.5 Limiti di Trading e Intermediazione). Con riguardo all'operatività sul mercato primario, è prevista una specifica Norma Operativa che disciplina il processo di sottoscrizione delle nuove emissioni obbligazionarie e azionarie, sia con riferimento all'operatività in proprio della Banca sia con riferimento all'operatività per la clientela, con previsione di un sistema centralizzato in capo all'ufficio Capital Markets e obblighi di registrazione delle sottoscrizioni (NO 5.32 Emissioni).

La Banca ha previsto un assetto operativo per la propria operatività sui mercati finanziari parametrato e proporzionato rispetto alla natura dei servizi finanziari offerti alla clientela e alla limitata operatività per conto proprio. In particolare, la Banca ha disposto una centralizzazione dell'esecuzione delle operazioni sui mercati in capo all'ufficio Capital Markets nell'ambito dell'Area Capital Market (fatta eccezione per le sottoscrizioni e i riscatti dei fondi d'investimento, che sono effettuate dall'ufficio Titoli, nonché per l'operatività dell'Area Asset Management come Investor Manager, che è effettuata tramite broker selezionati). L'accesso all'ufficio Capital Markets è generalmente riservato ai Collaboratori della Banca, salvo in casi eccezionali per i quali a favore di clienti o intermediari finanziari specifici è concessa un'autorizzazione all'accesso diretto all'ufficio Borsa (previa verifica dei relativi requisiti, come previsto dalla Norma Operativa 5.31 Ordini di borsa). In conformità con la Circolare FINMA 2013/8, la Direzione Generale valuta annualmente i rischi di abuso di mercato della Banca e definisce le eventuali misure correttive di carattere organizzativo. In particolare, la N.O. 4.3 Conti dei Collaboratori definisce sulla base di un Risk Assesment le varie categorie di rischi dei collaboratori; la Direzione Generale procede annualmente a verificare quali gruppi di Collaboratori potrebbero avere accesso o essere coinvolti nello sfruttamento d'informazioni privilegiate o nell'attività di manipolazione del mercato e a valutarne la relativa esposizione al rischio. Sulla base dei risultati di tale valutazione di rischio, viene esaminato se vi sono in essere misure organizzative adeguate atte a mitigare i rischi rilevati in ottemperanza a quanto previsto nella Circolare FINMA 2013/8 e sono predisposte dalla Banca misure di mitigazione qualora siano individuati dei gap.

a). Principi generali di comportamento

Si prevede un generale divieto per ogni Destinatario di tenere qualsiasi condotta di abuso di informazioni privilegiate nonché di manipolazione del mercato.

Tale divieto è ribadito anche dalla Norma Operativa disciplinante l'operatività svolta per conto proprio dai Collaboratori e membri del Consiglio di Amministrazione della Banca, sia nell'ambito dei rapporti bancari con la Banca, sia nell'ambito di rapporti in essere con altri istituti (NO 4.3 Conti dei Collaboratori), con particolare riferimento alle fattispecie di abuso di informazioni privilegiate. Si richiama, nella stessa Norma Operativa, il divieto di tenere condotte di abuso di informazioni

privilegiate anche nella forma del c.d. *front* e *parallel running* (ossia, sfruttamento delle informazioni confidenziali sulle transazioni dei clienti per trarne vantaggio effettuando operazioni in anticipo, in contemporanea ovvero immediatamente successive a quelle dei clienti), richiamando in particolare quanto disposto nella N.O. 5.83 Regole di condotta sul mercato. L'esecuzione di operazioni da parte dei Collaboratori, per conto proprio replicativi degli ordini di clienti prima, parallelamente o dopo l'esecuzione degli stessi, ovvero l'inserimento di transazioni per conto proprio tra singole tranche di ordini di clienti che non possono essere eseguiti in un'unica soluzione costituisce, inoltre, violazione dell'obbligo di diligenza e lealtà (cfr. N.O. 4.3 Conti dei collaboratori e 5.83 Regole di condotta sul mercato).

Sono previsti, inoltre, controlli periodici sulle operazioni personali effettuate, sotto la responsabilità dell'unità di Legal & Compliance per quanto riguarda le operazioni dei membri del Consiglio di Amministrazione e per tutti gli altri Collaboratori, , e sotto la responsabilità dell'unità Internal Audit per il Chief Risk Officer e i Collaboratori dell'unità Legal & Compliance .

Conformemente alla Norma Operativa Market Abuse, tutte le operazioni su strumenti finanziari (come definiti anche ai sensi della MAR) devono avere una giustificazione economica e corrispondere a un meccanismo di domanda e offerta, essendo vietato effettuare transazioni fittizie, ordini fittizi, operazioni (o introduzione di ordini) allo scopo di dare l'impressione di un'attività di mercato o di alterare la liquidità, il corso di borsa o la valutazione di strumenti finanziari. Sono, in particolare, vietate tutte le condotte che costituiscono esempi di manipolazione del mercato, come anche rappresentate dalla Circolare FINMA 2013/8.

Per quanto attiene alla fattispecie di c.d. manipolazione informativa, la Norma Operativa Market Abuse prevede un divieto per ciascun Destinatario di diffondere pubblicamente informazioni di cui sa o deve sapere che forniscono segnali falsi o fuorvianti in merito all'offerta, alla domanda o al corso di strumenti finanziari.

b). Segnalazione di operazioni sospette

Ai sensi della Norma Operativa Market Abuse, i Collaboratori, qualora riscontrassero indizi manifesti di abuso di mercato nell'ambito dell'operatività per conto della clientela, devono:

- appurarne le cause e, all'occorrenza, rinunciare a partecipare a tali operazioni.
- fare *escalation* della fattispecie al Responsabile della funzione Legal & Compliance (o al Responsabile della Revisione Interna, nel caso in cui la fattispecie coinvolga direttamente o indirettamente un membro della funzione Legal & Compliance), mediante notifica scritta e circostanziata.

Tutte le operazioni che, in ragione di indizi manifesti, potrebbero non essere compatibili con la normativa in materia di abusi di mercato devono essere documentate in maniera approfondita per escludere qualsiasi abuso.

La funzione Legal & Compliance (ovvero la Revisione Interna, a seconda dei casi), avvalendosi delle proprie competenze e informazioni, e con il supporto di tutte le ulteriori competenze interne alla Banca, valuta tempestivamente la fattispecie e si pronuncia formalmente in merito alla sussistenza o meno di una situazione di sfruttamento di informazioni privilegiate o di manipolazione del mercato, informandone il Collaboratore che ha avviato l'*escalation*.

I processi di *escalation*, di analisi e decisionale sono adeguatamente documentati dalla funzione Legal & Compliance (rispettivamente Revisione Interna) che ne conserva le evidenze.

Ove richiesto ai sensi della normativa applicabile, la funzione Legal & Compliance è tenuta ad effettuare una segnalazione di operazione sospetta all'Autorità competente (MROS), come previsto ai sensi della Norma AML (cfr. Sezione 7 della Parte Speciale del Modello).

c). Barriere informative (Chinese walls) / perimetri di riservatezza

La Banca gestisce le informazioni confidenziali atte a modificare l'andamento delle negoziazioni nell'ambito di perimetri di riservatezza con lo scopo di identificare ed impedire abusi, conflitti di interesse e danni ai clienti. Solo le persone all'interno delle aree di riservatezza hanno accesso alle informazioni confidenziali e la Banca adotta misure preventive adeguate affinché non vi sia alcun abuso dalla conoscenza di informazioni confidenziali. In particolare, è previsto un sistema di accesso riservato ai sistemi informatici e alle informazioni confidenziali sulla base dei principi "need to know" / "need to have" e sono definite linee gerarchiche con lo scopo di assicurare un'adeguata segregazione ed evitare eventuali situazioni di conflitto.

La Banca ha istituito, inoltre, una separazione gerarchica dell'area Asset Management da quella di Execution e Trading nonché una segregazione logistica delle aree riservate alle stesse attività di Execution e Trading rispetto alle altre aree aziendali.

d). Watch List e Restricted List

La gestione delle informazioni privilegiate è organizzata e sorvegliata tramite una c.d. *Watch List* e una c.d. *Restricted List*, tenute a cura della funzione Legal & Compliance.

La Watch List contiene dati sulle informazioni privilegiate suscettibili di influenzare l'andamento delle negoziazioni in possesso della Banca.

Con la *Restricted List* vengono previsti e poi comunicati divieti o restrizioni relativi a specifiche attività operative, come divieti di operazioni su determinati valori mobiliari, il blocco di transazioni o le restrizioni nella pubblicazione di analisi finanziarie, il genere di attività limitata (ad es., operazioni per conto "nostro", per i collaboratori, per la clientela, ecc.). Le restrizioni all'operatività si realizzano anche mediante l'adozione nei sistemi di negoziazione di appositi blocchi informatici.

Qualora un Collaboratore venga, direttamente o indirettamente, a conoscenza di un'informazione privilegiata nell'ambito dell'attività lavorativa (per es. informazioni da clienti che hanno legami con società emittenti) o a fattori esterni (per es. informazioni recepite durante lo svolgimento di altri incarichi, pubblici o non, o nel contesto della vita privata) ne deve dare comunicazione immediata al responsabile della funzione Legal & Compliance o, in sua assenza, al suo sostituto.

La funzione Legal & Compliance valuterà se l'informazione rientra effettivamente nella definizione di informazione privilegiata e, se del caso, provvederà al suo inserimento nella *Watch List* o nella *Restricted List*.

L'iscrizione dell'informazione nella *Watch List* è comunicata dalla funzione Legal & Compliance al funzionario che è a conoscenza dell'informazione privilegiata. Qualora, per esigenze operative, l'informazione sia comunicata ad altre persone all'interno della Banca, la cerchia di persone interessate verrà inserita nella Watch List.

L'iscrizione dell'informazione nella *Restricted List* è comunicata dalla funzione Legal & Compliance alle persone coinvolte (principalmente nelle unità Borsa, Asset management e Private banking).

A seconda del tipo di misure adottate, la funzione Legal & Compliance si avvarrà del supporto del responsabile della Revisione Interna (per il monitoraggio delle operazioni dei membri del Consiglio di Amministrazione) e del Risk Management (per il monitoraggio delle operazioni in conto proprio della Banca).

e). Registrazione e archiviazione delle telefonate e della corrispondenza

Tutte le conversazioni telefoniche (anche tramite telefoni cellulari) e la corrispondenza elettronica (come ad esempio, le e-mail e la messaggistica Bloomberg) dei Collaboratori attivi nelle operazioni su strumenti finanziari sono registrate e conservate per un periodo minimo.

Periodicamente è verificato il perimetro dei Collaboratori le cui conversazioni telefoniche sono soggette a registrazione.

Per i Collaboratori coinvolti, è vietato l'utilizzo di mezzi di comunicazione al di fuori di quelli messi a disposizione dalla Banca ed è altresì vietato l'utilizzo della messaggistica (quali SMS, MMS, Whatsapp, altro) sui telefoni cellulari.

f). Formazione

Copia della Norma Operativa Market Abuse è consegnata a cura dell'ufficio Risorse Umane a tutti i nuovi collaboratori assunti, i quali ne confermano la ricezione.

Sono organizzate sessioni formative specifiche in materia di abusi di mercato per tutti i nuovi Collaboratori, nonché sessioni periodiche per tutti i Collaboratori.

7. Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e autoriciclaggio (art. 25-octies) e reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater)

Il presente Capitolo della Parte Speciale si riferisce alle seguenti categorie di Reati previste dal D.Lgs. 231/2001:

a. "*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*" di cui all'art. 25 octies del D.Lgs. 231/2001.
b. "*Delitti con finalità di terrorismo o di eversione dell'ordine democratico*" di cui all'art. 25 quater del D.Lgs. 231/2001.

Le suddette categorie di Reati vengono trattate unitamente nel presente Capitolo della Parte Speciale poiché la prevenzione degli stessi avviene attraverso presidi analoghi.

7.1. Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e autoriciclaggio (art. 25-octies)

Il D.Lgs. n. 231/2007 (il "**Decreto Antiriciclaggio**"), nel dare attuazione in Italia alla Direttiva 2005/60/CE in materia di antiriciclaggio, ha introdotto nel D.Lgs. 231/2001 l'art. 25-*octies*, con il quale si estende la responsabilità amministrativa degli Enti ai reati di ricettazione, riciclaggio e impiego illecito di denaro, beni o utilità (in particolare, anche nel caso in cui tali fattispecie non siano commesse con finalità di terrorismo o di eversione dell'ordine democratico, che erano già contemplate dal D.Lgs. 231/2001 dall'art. 25-*quater*).

Successivamente, la L. 186/2014 ha introdotto nel codice penale la nuova fattispecie di reato di autoriciclaggio (art. 648-*ter* c.p.), prevedendo contestualmente l'estensione di tale stessa fattispecie ai reati presupposto previsti dall'art. 25-*octies* del D.Lgs. 231/2001.

Da ultimo, il D.lgs. 8 novembre 2021, n. 195, in attuazione della Direttiva Europea 2018/1673 sulla lotta al riciclaggio mediante il diritto penale, ha esteso la punibilità dei reati di cui agli artt. 648 c.p. ("Ricettazione"), 648-bis c.p. ("Riciclaggio"), 648-ter c.p. ("Impiego di beni o utilità di provenienza illecita") e 648.ter.1 c.p. ("Autoriciclaggio") ai casi in cui il denaro o le cose oggetto del reato provengano – non solo da delitto ma anche - da contravvenzione.

L'oggetto materiale dei reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e di autoriciclaggio è costituito da qualsiasi entità economicamente apprezzabile (ad es., denaro, i titoli di credito, mezzi di pagamento, metalli preziosi) proveniente da delitto o da contravvenzione, ossia che ne sia:

- prodotto (risultato, frutto ottenuto dal colpevole con la commissione del reato);
- profitto (lucro o vantaggio economico ricavato dal reato); o
- prezzo (compenso dato per indurre, istigare, determinare taluno alla commissione del reato)

Può dare origine ad un prodotto/profitto proveniente da delitto o contravvenzione anche un reato in materia fiscale, come il caso di un reato di frode (ad es. utilizzo di fatture per operazioni inesistenti che determinino un fittizio credito Iva da detrarre) e di omessa o infedele dichiarazione di redditi per importo oltre le soglie di rilevanza penale.

Per quanto riguarda l'aspetto soggettivo, la punibilità dei reati in oggetto richiede la consapevolezza della provenienza illecita del bene. Seguendo un'interpretazione rigorosa della norma, sarebbe

sufficiente anche l'aver agito nel dubbio della provenienza illecita, accettandone il rischio (cosiddetto dolo indiretto od eventuale). Pertanto, la presenza in determinate situazioni concrete di indici di anomalia o di comportamenti anomali potrebbe essere ritenuta una circostanza oggettiva grave ed univoca atta a far sorgere il dubbio dell'illecita provenienza del bene.

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

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

La Banca è soggetta a specifici obblighi di contrasto del riciclaggio e del finanziamento del terrorismo ai sensi della normativa svizzera (di seguito, gli "**Obblighi Antiriciclaggio**") (6). Essendo la Svizzera un Paese aderente al GAFI-FAFT, tali Obblighi Antiriciclaggio si considerano "equivalenti" a quelli adottati dall'Italia in applicazione delle Direttive Europee e pertanto idonei a prevenire i reati oggetto della presente Parte Speciale ([7]).

La violazione degli Obblighi Antiriciclaggio, nell'ambito dell'applicazione del Modello, potrebbe esporre la Banca al rischio di commissione di reati di riciclaggio e di finanziamento del terrorismo e quindi all'imputazione della responsabilità amministrativa ex Decreto 231/01. Ai fini dell'imputazione di tale responsabilità è necessario che la violazione degli Obblighi Antiriciclaggio

([6]) Si richiamano, in particolare le seguenti disposizioni normative di diritto svizzero e di autodisciplina in materia di prevenzione del riciclaggio e del finanziamento del terrorismo applicabili alla Banca:

- il Codice Penale Svizzero ("**CPS**"), artt. 305bis, 305ter e 260quinquies;
- la "*Legge federale relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo*" del 10 ottobre 1997 aggiornata dalla Legge federale concernente l'attuazione delle raccomandazioni GAFI del 12 dicembre 2014;
- la "*Ordinanza relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo*" dell'11 novembre 2015;
- la "*Ordinanza dell'Autorità federale di vigilanza sui mercati finanziari sulla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo nel settore finanziario*" (la c.d. Ordinanza FINMA sul riciclaggio di denaro) del 3 giugno 2015;
- la "*Convenzione relativa all'obbligo di diligenza delle banche*" (CDB 20), sottoscritta tra l'Associazione Svizzera dei Banchieri («ASB») da una parte e le principali banche svizzere (ultima edizione del 13 giugno 2018).

In particolare, ai sensi del diritto svizzero, sono punibili le seguenti condotte:

1) art. 305 bis del CPS sul riciclaggio di denaro: è punibile chiunque compie un atto suscettibile di vanificare l'accertamento dell'origine, il ritrovamento o la confisca di valori patrimoniali, sapendo o dovendo presumere che provengono da un crimine ai sensi dell'art. 10 cpv. 2 CP o da un delitto fiscale qualificato.
   Per "*delitto fiscale qualificato"* si intende la condotta punita ai sensi dell'art. 186 della Legge Federale sull'imposta federale diretta del 14 dicembre 1990 e successive integrazioni e modificazioni, ossia: "1. *Chiunque, per commettere una sottrazione d'imposta ai sensi degli articoli 175–177, fa uso, a scopo d'inganno, di documenti falsi, alterati o contenutisticamente inesatti, quali libri contabili, bilanci, conti economici o certificati di salario e altre attestazioni di terzi, è punito con una pena detentiva sino a tre anni o con una pena pecuniaria. Oltre alla pena condizionalmente sospesa il giudice può infliggere una multa sino a 10 000 franchi. 2. È salva la pena per sottrazione d'imposta. 3. In caso di autodenuncia ai sensi degli articoli 175 capoverso 3 o 181a capoverso 1, si prescinde dall'aprire un procedimento penale per tutti gli altri reati commessi allo scopo della sottrazione d'imposta di cui si tratta. La presente disposizione è applicabile anche ai casi di cui agli articoli 177 capoverso 3 e 181a capoversi 3 e 4*"
2) art. 305ter del CP svizzero sulla carente diligenza nell'identificazione, che punisce chiunque non identifichi l'avente diritto economico con la diligenza richiesta dalle circostanze;
3) Art. 260quinquies CP sul finanziamento del terrorismo che punisce chi raccoglie o mette a disposizione valori patrimoniali nell'intento di finanziare atti di violenza criminali volti ad intimidire la popolazione o a costringere uno Stato o un'organizzazione internazionale a fare o omettere un atto

([7]) Si richiamano a tal riguardo il "*Mutual Evaluation Report of Switzerland, 2016*" e il successivo "*Follow Up Report Switzerland January 2020*", entrambi rilasciati dal FAFT.

sia caratterizzata dalla volontà di coprire l'operazione di riciclaggio o di finanziamento al terrorismo del cliente, in quanto in tale ipotesi la Banca concorrerebbe nella commissione del reato da parte del cliente stesso (ad es., dolosa mancata segnalazione di operazione sospetta alle autorità di vigilanza). A tal fine, quindi, rileva la corretta gestione dei processi previsti dalla Banca e del Gruppo in conformità alla normativa applicabile in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

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

7.1.1. Ricettazione (648 c.p.)

Commette il reato di ricettazione chiunque, allo scopo di procurare a sè o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto o da una contravvenzione punita con l'arresto superiore nel massimo a un anno e nel minimo a sei mesi, alla cui commissione non ha partecipato, o comunque si intromette nel farli acquistare, ricevere od occultare.

Per tale reato è richiesta la presenza di dolo specifico da parte di chi agisce, e cioè la coscienza e la volontà di trarre profitto, per sé stessi o per altri, dall'acquisto, ricezione od occultamento di beni di provenienza illecita. E', inoltre, richiesta la conoscenza della provenienza illecita del denaro o del bene; la sussistenza di tale elemento psicologico potrebbe essere riconosciuta in presenza di circostanze gravi ed univoche - quali ad esempio la qualità e le caratteristiche del bene, le condizioni economiche e contrattuali inusuali dell'operazione, la condizione o la professione del possessore dei beni - da cui possa desumersi che nel soggetto che ha agito poteva formarsi la certezza della provenienza illecita del denaro o del bene.

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

Commette il reato di riciclaggio chiunque soggetto, che non abbia concorso alla commissione del delitto sottostante, sostituisca o trasferisca denaro, beni od altre utilità provenienti da un delitto o da una contravvenzione punita con l'arresto superiore nel massimo a un anno e nel minimo a sei mesi, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Questa fattispecie è volta a punire coloro che - consapevoli della provenienza illecita di denaro, beni o altre utilità - compiano le operazioni descritte, in maniera tale da creare in concreto difficoltà alla scoperta dell'origine illecita dei beni considerati. Ai fini del perfezionamento del reato non rileva se il soggetto ha agito per conseguire un profitto o con lo scopo di favorire gli autori del reato sottostante ad assicurarsene il provento.

Costituiscono riciclaggio le condotte dinamiche, atte a mettere in circolazione il bene, mentre la mera ricezione od occultamento potrebbero integrare il reato di ricettazione. Con riferimento ai rapporti bancari, anche la semplice accettazione di un deposito potrebbe integrare la condotta di sostituzione tipica del riciclaggio (sostituzione del denaro contante con moneta scritturale, quale è il saldo di un rapporto di deposito). Come per il reato di ricettazione, la consapevolezza dell'agente in ordine alla provenienza illecita può essere desunta da qualsiasi circostanza oggettiva grave ed univoca.

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

Commette il reato in esame qualsiasi soggetto che impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto o da una contravvenzione punita con l'arresto superiore nel massimo a un anno e nel minimo a sei mesi, fuori dei casi di concorso nel reato d'origine e dei casi previsti dagli articoli 648 (ricettazione) e 648-*bis* (riciclaggio) c.p..

Rispetto al reato di riciclaggio, pur essendo richiesto il medesimo elemento soggettivo della conoscenza della provenienza illecita dei beni, l'art. 648 *te*r circoscrive la condotta all'impiego di tali risorse in attività economiche o finanziarie.

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

Risponde del reato di autoriciclaggio chi, avendo commesso o concorso a commettere un qualsiasi delitto o da una contravvenzione punita con l'arresto superiore nel massimo a un anno e nel minimo a sei mesi dal quale provengono denaro, beni, o altre utilità, su tali proventi compie operazioni di impiego, sostituzione o trasferimento in attività economiche, finanziarie, imprenditoriali o speculative, con modalità tali da ostacolare concretamente l'identificazione della loro provenienza illecita.

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

7.2. Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater)

L'art. 25-quater, comma 1, del Decreto dispone la punibilità dell'Ente, ove ne sussistano i presupposti, nel caso in cui siano commessi, nell'interesse o a vantaggio dell'Ente stesso, "*delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali*".

La norma non prevede un elenco di reati chiuso e tassativo, ma si riferisce ad un qualsivoglia illecito penale caratterizzato dalla particolare finalità di terrorismo o di eversione dell'ordine democratico perseguita dal soggetto agente. Tenuto anche conto dell'operatività della Banca, può venire, così, in rilievo una pluralità di fattispecie criminali, come, a titolo esemplificativo:

- il "*finanziamento di condotte con finalità di terrorismo*" (art. 270-quinquies.1 c.p.);
- il reato di cui all'art. 270-bis c.p., denominato "*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*", che punisce "*chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratic*o".

Il comma 4 dello stesso art. 25-quater del Decreto dispone, inoltre, la punibilità dell'Ente "*in relazione alla commissione di delitti, diversi da quelli indicati nel comma 1, che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999*".

7.3. Attività aziendali sensibili

Il rischio che si verifichino nel contesto bancario i reati oggetto della presente Sezione di Parte Speciale (ossia, ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio e delitti con finalità di terrorismo o di eversione dell'ordine democratico) è soprattutto connesso ai rapporti della Banca con la clientela e ad ipotesi di coinvolgimento/concorso in attività criminose della stessa.

Le Attività aziendali sensibili sono quelle coinvolte nelle seguenti attività:

- instaurazione e gestione dei rapporti con la clientela (apertura e gestione di servizi di private banking);
- trasferimento/accettazione di fondi/valori;
- accettazione e consegna di averi fisici (ad esempio, contante, titoli fisici, metalli preziosi e carte valori).

Con specifico riferimento all'autoriciclaggio, sono state individuate inoltre le seguenti Attività Sensibili:

- attività transfrontaliere in Italia;
- gestione dei fondi propri della Banca.

Con riguardo alle Attività Sensibili ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché delitti con finalità di terrorismo o di eversione dell'ordine democratico le Unità organizzative ed i comitati della Banca principalmente coinvolti sono:

- Consiglio di Amministrazione;
- Audit & Risk Committee;
- Direzione Generale;
- Comitato Accettazione Clienti;
- Comitato Rischi;
- Legal & Compliance;
- Private Banking;
- Corporate Banking.

Con specifico riferimento all'attività sensibile "*instaurazione e gestione dei rapporti con la clientela (apertura e gestione di servizi di private banking)"* possono essere coinvolti anche gli EAM ai quali sia stata conferita la "*delega dell'identificazione del contraente, dell'accertamento del detentore del controllo e la determinazione dell'avente diritto economico*". I presidi relativi alla suddetta attività sensibile sono quindi applicabili anche agli EAM.

Con riferimento all'autoriciclaggio si rinvia alle unità organizzative e ai comitati individuati nelle sezioni della presente Parte Speciale del Modello relative alla commissione dei reati presupposto ex D.Lgs. 231/2001 (reati contro la pubblica amministrazione, reati societari, i reati e illeciti amministrativi riconducibili ad abusi di mercato, reati informatici, reati tributari, reati di criminalità organizzata etc.).

In relazione alla possibilità che l'autoriciclaggio derivi dalla commissione di reati di abusivismo bancario e finanziario, sono state individuate inoltre le seguenti unità organizzative:

- *Consiglio di Amministrazione;*
- *Direzione Generale;*
- *private banking;*
- *corporate banking.*

7.4. Presidi procedurali e di controllo

Si riporta di seguito una descrizione dei presidi procedurali e di controllo adottati dalla Banca al fine di prevenire la commissione specifica dei reati oggetto della presente Sezione di Parte Speciale del Modello.

Tutti i protocolli del presente Modello, ancorché previsti in altre sezioni dello stesso, laddove tesi a prevenire il reimpiego di proventi derivanti dalla commissione di reati, si devono intendere predisposti anche al fine della prevenzione dei reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e di autoriciclaggio. Si richiamano soprattutto i protocolli relativi alle Aree sensibili concernenti i reati contro la pubblica amministrazione, i reati societari, i reati e illeciti amministrativi riconducibili ad abusi di mercato, i reati di criminalità organizzata e i reati tributari.

Con particolare riferimento alle Attività Sensibili al reato di autoriciclaggio - presupponendosi la commissione da parte della Banca (anche sotto forma di concorso) del reato da cui originano i proventi illeciti - si rinvia ai presidi e ai controlli adottati dalla medesima in relazione alla potenziale commissione di Reati Presupposto previsti nella Parte Generale e in altre sezioni della presente Parte Speciale. In particolare:

- relativamente alle "*attività cross-border*" verso l'Italia si richiamano i presidi e i controlli a prevenzione dei reati di abusivismo bancario e finanziario previsti nella Parte Generale del presente Modello (cfr. Sezione 2.1 della Parte Generale del presente Modello);
- in relazione alla "*gestione dei fondi propri della Banca*", la Banca rispetta le disposizioni normative alla medesima applicabili. Si richiamano inoltre i principi previsti dalla Parte Generale del Modello in materia di controlli interni (Sezione 2.7.2. della Parte Generale) e di deleghe e procure (Sezione 2.7.3. della Parte Generale del Modello) nonchèi presidi relativi ai reati societari (Cfr. Sezione 5 della Parte Speciale del presente Modello).

L'attività di prevenzione dei reati oggetto della presente Parte Speciale si basa, innanzitutto, sull'adozione di un sistema articolato di misure preventive e di controlli, nell'ambito del quale sono definiti in modo chiaro e specifico i diversi ruoli e responsabilità. Tale sistema di misure preventive e di controlli è disciplinato nelle policy e procedure interne adottate dalla Banca in ottemperanza alla normativa applicabile in tema di contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo ("**AML**").

In particolare, costituiscono parte integrante e sostanziale del presente protocollo le seguenti Policy e Norme Operative interne:

- Risk Appetite Framework Policy del Gruppo PKB ("**RAF**")
- Legal & Compliance Policy del Gruppo PKB ("**L&C Policy**")
- Norma Operativa n. 2.20 recante "*Lotta al riciclaggio di denaro e al finanziamento del terrorismo"* (di seguito "**Norma AML**");
- Norma Operativa n. 2.1. recante "*Apertura relazione d'affari clientela e gestione della documentazione di base obbligatoria"* (di seguito "**Procedura Apertura Rapporti d'Affari**");
- Norma Operativa 2.30 recante "*Relazioni clientela con persone esposte politicamente (PEP)*" (di seguito "**Procedura Relazioni PEP**");
- Norma Operativa 2.34 recante "*Intermediari Finanziari*";
- Norma Operativa 2.42 recante "*Conti Collettivi / Conti Transitori*";

- Norma Operativa 2.51 recante "*Relazioni d'affari con clienti domiciliati in paesi con limitazioni*";
- Norma Operativa 2.55 recante "*Conformità fiscale delle relazioni bancarie*";
- Norma Operativa 2.45 recante "*Prelevamenti e Versamenti per cassa*";
- Norma Operativa 5.52 *"Valori fisici in custodia presso PKB";*
- Norma Operativa 5.12 *"cassette di sicurezza".*

In particolare, la Banca ha identificato nell'ambito dei "*Rischi Legali e di Compliance*", contemplati nel Risk Appetite Framework Policy di Gruppo, i c.d. "*rischi legati ai crimini finanziari*", che consistono nel rischio di commissione dei reati di riciclaggio, finanziamento del terrorismo ed evasione fiscale nell'ambito delle attività svolte a favore della clientela Private e Corporate Banking c.d. "sofisticata", ossia che gestisce i propri averi anche attraverso strutture complesse e/o legate a centri *offshore.*

Rispetto all'insorgere e all'impatto dei suddetti rischi, la Banca - in qualità di capogruppo, responsabile della sorveglianza consolidata del Gruppo PKB secondo la regolamentazione FINMA - ha adottato nel proprio modello di *business* i seguenti principi relativamente all'appetito di rischio:

- il Gruppo instaura relazioni con clientela che rispetta la normativa fiscale applicabile ("Tax compliance");
- il Gruppo limita le relazioni con la clientela che potrebbero comportare un rischio accresciuto (ad esempio soggetti domiciliati in giurisdizioni non trasparenti o PEP);
- la clientela è sottoposta a un processo di accettazione che comporta una valutazione dettagliata preventiva e una rivalutazione periodica della clientela esistente;
- non è ammessa alcuna violazione consapevole della normativa interna ed esterna da parte dei collaboratori.

La gestione dei rischi legati a crimini finanziari trova, quindi, concreta espressione nella determinazione di un efficace quadro normativo interno e di un'adeguata organizzazione aziendale nonché nella relativa applicazione.

In particolare, i processi di gestione e sorveglianza del rischio "*Legale, reputazionale e di Compliance*" sono specificati nella L&C Policy, la quale definisce le responsabilità, gli strumenti utilizzati e i flussi informativi necessari a livello di Gruppo per assicurare un'adeguata gestione dei suddetti rischi nel perseguimento degli obiettivi di *business*.

La L&C Policy prevede in particolare che la Banca e le società controllare del Gruppo debbano:

- impedire che tramite le proprie relazioni clientela vengano immessi valori patrimoniali di origine criminale nel circuito finanziario legale, definendo nel proprio sistema di controllo interno una metodologia di *due diligence* volta ad assicurare l'applicazione dei propri doveri di diligenza in ambito di lotta contro il riciclaggio di denaro e prevenzione ai delitti fiscali perseguibili penalmente;
- identificare adeguatamente e rivalutare periodicamente la propria clientela, rispettivamente gli aventi diritto economico;
- limitare le relazioni con clientela che comporta un rischio accresciuto e con persone esposte politicamente (PEP), per le quali devono essere implementati degli obblighi accresciuti di chiarificazione complementare, di controllo e di monitoraggio;

- assicurare un monitoraggio adeguato della situazione politica/economica/normativa dei Paesi caratterizzati da un contesto generale turbolento e applicazione di una due diligence accresciuta nel seguire relazioni d'affari collegate a clientela domiciliata in paesi con limitazioni.

La Norma AML, ponendosi quale norma operativa interna, definisce i requisiti minimi di prevenzione del riciclaggio e finanziamento del terrorismo (di seguito "**AML**") della Banca e costituisce il modello di riferimento per le altre entità del Gruppo, salva l'applicazione delle specifiche disposizioni normative territorialmente applicabili. La Norma AML, pertanto - ove necessario - è integrata con procedure interne volte a recepire gli adempimenti specifici previsti dalle disposizioni normative e regolamentari locali.

La Norma AML detta specifici principi di comportamento e di controllo volti a mitigare il rischio di commissione dei reati di riciclaggio e finanziamento del terrorismo attraverso: 1) la definizione di processi di accurata selezione e conoscenza della clientela - sia in sede di c.d. *onboarding*, sia in via continuativa - 2) il monitoraggio delle operazioni poste in essere dalla stessa, 3) l'analisi e l'eventuale segnalazione alle autorità competenti delle operazioni ad alto rischio di riciclaggio o finanziamento del terrorismo (c.d. "AML HIT" e le c.d. "**Transazioni Inusuali**") nonché 4) l'adeguata formazione del personale addetto allo svolgimento di tali attività.

In particolare, la Norma AML definisce:

- le misure e i controlli in materia AML nell'ambito dei processi di apertura delle relazioni e nell'esecuzione delle transazioni da parte della clientela;
- i criteri e i processi di identificazione del cliente (c.d. "*titolare*") e del beneficiario effettivo (c.d. "*avente diritto economico*");
- i processi di classificazione dei clienti e dei beneficiari effettivi, in base al grado di esposizione al rischio di riciclaggio e finanziamento del terrorismo, nonché di analisi approfondita degli stessi attraverso la raccolta di specifiche informazioni, dati e documenti (c.d. "*Due Diligence*");
- i processi di accettazione del cliente attraverso un articolato sistema di autorizzazioni interne ("*escalation*") in base al profilo di rischio della clientela o dell'Avente Diritto Economico;
- le tipologie di relazioni e operazioni vietate;
- i processi di monitoraggio delle transazioni e dei trasferimenti di fondi posti in essere dalla clientela volti ad indentificare, automaticamente o manualmente, le transazioni a rischio superiore di riciclaggio o finanziamento del terrorismo (le c.d. "AML HIT" e le c.d. "Transazioni Inusuali") per le quali sono previsti ulteriori specifici processi di analisi e approfondimento;
- i processi di monitoraggio della clientela, attraverso la consultazione delle *black lists* in materia di antiriciclaggio;
- i processi di rivalutazione periodica delle relazioni e di conseguente aggiornamento del profilo di rischio della clientela;
- i processi di segnalazione all'autorità competente ("**MROS**") delle transazioni per le quali, a seguito di approfondite analisi, sia emerso il fondato sospetto di riciclaggio;

Nell'ambito dei suddetti processi la Norma AML:

- individua le funzioni addette allo svolgimento delle attività e dei relativi controlli sulle stesse, nel rispetto del principio di segregazione dei ruoli tra soggetti che effettuano i controlli e coloro che sono oggetto dei controlli stessi;

- disciplina lo svolgimento "ordinario" di ciascun processo nonché le variazioni applicabili ai casi eccezionali o specifici, prevedendo anche in tali casi specifici processi di escalation;
- disciplina per ciascun processo i controlli di primo livello, c.d. di linea, e i controlli di secondo livello.

a) Il sistema di governance e di controlli interni in materia di lotta contro il riciclaggio e il finanziamento del terrorismo

La Banca ha adottato un articolato sistema organizzativo di *governance* e di controlli interni finalizzato ad individuare e gestire il rischio di riciclaggio e finanziamento del terrorismo all'interno della Banca e del Gruppo.

In particolare, la Banca ha attribuito ai diversi organi e funzioni aziendali, nel rispetto del principio di segregazione, specifici ruoli e responsabilità di attuazione delle misure di prevenzione e di controllo previste dalle policy e procedure aziendali in materia di lotta contro il riciclaggio e finanziamento del terrorismo.

Si riporta qui di seguito una rappresentazione schematica dei ruoli e responsabilità che sono stati attribuiti agli organi, ai comitati interni e alle unità organizzative della Banca al fine di adempiere agli obblighi antiriciclaggio, sia in qualità di società capogruppo, responsabile della sorveglianza consolidata del Gruppo PKB secondo la regolamentazione FINMA, sia come istituto bancario.

ORGANO/FUNZIONE	**RUOLI E RESPONSABILITA'**
Consiglio di Amministrazione:	Definisce le strategie e le politiche applicabili in materia di antiriciclaggio e contrasto del finanziamento del terrorismo; in particolare, emana le linee guida necessarie a livello di Gruppo, assicurandone l'esecuzione da parte della Direzione Generale e degli organi competenti delle affiliate, affinché il Gruppo rispetti costantemente le disposizioni in materia AML. Approva e rivede annualmente le soglie di appetito di rischio (Risk Appetite) e le relative deviazioni tollerate (Risk Tolerance) sempre nel rispetto dei limiti di Risk Capacity.
Direzione Generale	Nell'ambito della gestione operativa della Banca è responsabile dell'attuazione del sistema di gestione e di controllo dei rischi in materia AML.
Comitato Rischi (CORI)	Il CORI è responsabile di garantire una visione integrata e di insieme di tutti i rischi del Gruppo e di monitorare la loro aderenza all'appetito di rischio definito dal CA. Con riferimento ai suddetti ambiti di competenza, il CORI ha la funzione di: - identificare, misurare, controllare e monitorare i rischi su base individuale e consolidata; - definire e controllare contenuto e tempistica della reportistica che le varie entità, rientranti nel perimetro di sorveglianza consolidata, devono produrre al fine di consentire un adeguato monitoraggio dei rischi su base consolidata; - approvare i metodi di controllo dei rischi e dei limiti;

	- monitorare l'adesione della Banca a leggi, regolamenti e comunicazioni interpretative delle Autorità di Vigilanza; - individuare la necessità di interventi e sollecitare soluzioni agli uffici competenti; - allestire e trasmettere trimestralmente agli organi sociali competenti un rapporto sull'andamento generale dei rischi sopra indicati e sulla loro gestione; - analizzare e trasmettere agli organi sociali competenti rapporti e informazioni sulle tematiche rilevanti di compliance/AML.
Comitato Accettazione Clientela ("**CAC**")	E' incaricato di valutare l'apertura e il mantenimento di relazioni che, nell'ambito delle procedure AML, richiedono criteri di *escalation*. Valuta, inoltre, le eventuali iniziative delle entità del Gruppo in relazione al processo di apertura delle relazioni bancarie al fine di assicurare un approccio omogeneo.
Chief Risk Officer ("**CRO**")	Il CRO è responsabile verso il Consiglio di Amministrazione dell'implementazione del *framework* riguardante l'appetito, il controllo e il *reporting* di i rischi ai quali è esposto il Gruppo, tra cui, nell'ambito dei rischi Legale e di Compliance, il rischio di riciclaggio e finanziamento del terrorismo.
Legal & Compliance ("**L&C**")	La funzione L&C, costituisce la seconda linea di difesa nell'ambito dei presidi AML e - in conformità a quanto previsto dall'ordinanza FINMA sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo - è stata individuata quale "*servizio interno qualificato di lotta contro il riciclaggio*". In tale veste la Funzione L&C: • verifica l'osservanza delle disposizioni di legge e della normativa interna nell'ambito della lotta contro il riciclaggio di denaro e il finanziamento del terrorismo; • analizza e aggiorna con cadenza trimestrale i rischi in materia AML sulla base di specifici "*Risk Indicators*", "*Minimum Standards & Key Controls*", e report (es. "*Top 10 Legal Cases*"). Tale analisi è condotta sia a livello di Gruppo, sia delle singole entità e i relativi esiti sono riportati a CRO; • definisce gli strumenti di mitigazione del rischio legale e di compliance in materia AML; • pianifica la formazione interna in materia AML; • analizza e comunica alle autorità competenti le operazioni sospette di riciclaggio o finanziamento del terrorismo. L'ufficio L&C della Banca ("Group L&C") è responsabile della sorveglianza consolidata del rischio "*legale, reputazionale e di compliance*" del Gruppo. Gli uffici locali L&C delle entità controllate italiane ("**LCO**") sono subordinati gerarchicamente al consiglio di amministrazione dell'entità stessa e, ai fini della sorveglianza consolidata, riportano al responsabile del Group L&C ("**HLC**"). Il Group L&C dipende direttamente dal Chief Risk Officer di Gruppo (CRO).
Revisione Interna ("**Internal Audit**")	• esamina e valuta in maniera indipendente, data l'esposizione e la propensione al rischio della Banca, l'efficacia e l'efficienza dei

	processi di gestione dei rischi nonché del sistema di governance e di controllo interno in materia AML; • verifica il rispetto delle normative vigenti (interne ed esterne) in materia di AML, sia a livello di Banca che di Gruppo; • garantisce un sistema appropriato di *reporting* delle raccomandazioni rilevate e di *follow up* per la risoluzione delle stesse; • verifica la rimozione delle anomalie riscontrate.
Private Banking e Corporate Banking	Le funzioni Private banking e Corporate Banking costituiscono le prime linee di difesa nell'ambito del sistema dei controlli interni in materia AML. In particolare, nell'ambito di tali divisioni sono individuate figure professionali (Relationship Manager, Capo Team del Relationship Manager, Capo Area, Capo Divisione 1 o 2) che, con diversi ruoli e responsabilità in materia AML, partecipano al processo di apertura e monitoraggio delle relazioni d'affari con la clientela e di gestione della documentazione di base obbligatoria. Le suddette figure partecipano ai diversi livelli dei processi di *escalation* previsti dalla Norma AML e dalla Procedura Apertura Rapporti d'Affari. Nell'ambito delle funzioni Private Banking e Corporate Banking, le attività di individuazione e raccolta dati, informazioni e documenti della clientela sono demandate ai Relationship Managers.

Fermo restando che tutte le unità organizzative della Banca e delle singole entità del Gruppo sono responsabili di assicurare il rispetto della normativa interna ed esterna vigente, la specifica gestione e mitigazione dei "*rischi legati ai crimini finanziari*" è effettuata tramite un articolato sistema di controlli interni in materia AML, basato su tre linee di difesa:

- la prima linea di difesa, attribuita alle funzioni Private Banking e Corporate Banking, è proprietaria del rischio ed è responsabile della relativa gestione; inoltre è responsabile dell'allineamento delle proprie attività alla strategia ed all'appetito di rischio definito dal Consiglio di Amministrazione della Banca;
- la seconda linea di difesa, attribuita a L&C, è responsabile della definizione degli *standard* di rischio e di controllo, e verifica, tramite l'esecuzione di controlli indipendenti, l'efficacia della gestione del rischio da parte della prima linea di difesa;
- la terza linea di difesa, attribuita alla funzione Internal Audit, è responsabile di fornire una conferma indipendente relativamente all'efficacia del *framework* normativo e applicativo interno a supporto della gestione dei rischi e controlli in materia AML.

Il sistema di controlli interni in materia AML si basa inoltre sui principi generali stabiliti nel "*Regolamento sul sistema di controllo interno del gruppo PKB*" adottato dalla Banca, ossia:

1) "*Principio dei quattro occhi*" viene perseguito attraverso la suddivisione delle attività/responsabilità relative ai processi AML tra differenti funzioni ("*segregation of duties*"), nonché attraverso lo svolgimento di verifiche incrociate e di duplici controlli;
2) Identificazione delle responsabilità delle informazioni e dei processi (*"accountability*"), al fine di definire le responsabilità nei confronti degli organi superiori;

3) Tracciabilità (e non ripudiabilità) dei dati e delle informazioni, al fine di rendere attendibile, ricostruibile e valutabile le attività e i processi in ambito AML;
4) Identificazione continua delle anomalie (elementi e processi non conformi) e delle relative misure correttive al fine di mitigare gli errori e le anomalie nonché di migliorare i processi.

b) Principi generali di comportamento

In via preliminare, la Norma AML identifica le tipologie di rapporti per i quali la Banca prevede un generale divieto di instaurazione del rapporto con il cliente, nonché le tipologie di operazioni che in generale la Banca vieta di eseguire.

E' fatto divieto a tutti i Dipendenti della Banca di accettare beni patrimoniali dei quali si sappia o si possa supporre la provenienza criminosa, indipendentemente da dove sia stato compiuto il crimine o se il medesimo configuri un c.d. "*delitto fiscale qualificato*".

In particolare, a titolo esemplificativo e non esaustivo, sono vietate:

- le relazioni che si riferiscano a rapporti commerciali con imprese o persone di cui si sappia o si possa supporre che costituiscano o facciano parte, sostengano o finanzino un'organizzazione criminale o terroristica;
- le relazioni che fanno capo a rapporti con banche che non hanno una presenza fisica nello Stato secondo il diritto del quale sono organizzate (c.d. banche fittizie o Shell Banks);
- le operazioni che comportino un rischio eccessivamente elevato (ad esempio, quando un non-cliente consegna valori patrimoniali per la rimessa ad un altro non-cliente; oppure custodire patrimoni di un non-cliente sapendo o potendo presumere che provengano da un'attività criminosa o da delitto fiscale qualificato).

c) Presidi in relazione all'apertura di nuovi rapporti: verifica dell'identità della clientela, classificazione della clientela e due diligence

La Norma AML prevede che l'instaurazione di qualsiasi rapporto d'affari con la clientela sia subordinato allo svolgimento di accurati processi di identificazione, classificazione e *due diligence*, al fine di comprendere il potenziale rischio di riciclaggio e finanziamento del terrorismo nell'ambito delle attività di *on-boarding* della clientela e di successiva gestione della stessa.

Con particolare riferimento ai processi di identificazione e verifica della clientela, la Norma AML dispone che i medesimi si basino su:

- la raccolta accurata e completa di dati, informazioni e documenti in relazione a ciascun soggetto rilevante del rapporto (c.d. "*Titolare*", "*Avente Diritto Economico*", "*Pagatore*", "*Detentore del Controllo*" etc.) al fine di identificare e conoscere la clientela sin dalla prima fase di instaurazione del rapporto contrattuale. Tale raccolta avviene a cura del Relationship Manager attraverso la compilazione da parte di tutti i soggetti interessati di un profilo Know Your Customer (c.d. "**KYC**");
- l'individuazione del titolare effettivo (c.d. "*Avente Diritto Economico*") di ciascun rapporto, ossia delle persone fisiche o giuridiche che godono in ultima istanza dei benefici economici derivanti dagli asset depositati, gestiti o amministrati dalla Banca;
- la registrazione di tutti i dati, informazioni e documenti nel sistema informativo specificamente adottato dalla Banca per la gestione degli adempimenti AML;

- il monitoraggio e l'aggiornamento dei dati e delle informazioni raccolte durante tutta la vigenza del rapporto in essere con la Banca.

La Banca può delegare le operazioni di identificazione del contraente, accertamento del detentore del controllo e determinazione dell'avente diritto economico a soggetti terzi (nello specifico agli EAM). Con riferimento a tali casi, la Banca ha adottato i seguenti presidi (Cfr. Norma Operativa 2.34 Intermediari Finanziari):

- all'EAM è attribuita una specifica delega all'adempimento dei suddetti obblighi AML, nell'ambito della quale sono specificamente indicati compiti e responsabilità
- la concessione della delega è soggetta ad uno specifico processo autorizzativo interno;
- è vietata la subdelega a soggetti terzi;
- la delega è concessa solo a persone fisiche e ove l'EAM sia strutturato in forma societaria nell'accordo di delega sono identificate le persone fisiche addette allo svolgimento delle attività AML per conto della Banca. Tutte le persone fisiche delegate sono registrate in un'apposita lista tenuta dalla Banca;
- tutti i soggetti delegati sono obbligati a completare uno specifico percorso formativo organizzato dalla Banca e debitamente documentato.

La Banca pone in essere specifici controlli sull'operato dei soggetti delegati.

La Norma AML prevede inoltre un processo di classificazione della clientela basato sul livello di esposizione di ciascun cliente al rischio di commissione del reato di riciclaggio e finanziamento del terrorismo. Con particolare riferimento alla classificazione della clientela sono stabiliti i seguenti principi:

- al momento dell'instaurazione del rapporto contrattuale ciascun cliente è inquadrato nell'ambito di specifiche classi di rischio, definite dal sistema informatico sulla base di un algoritmo che tiene conto di una serie di fattori di rischio preimpostati. Sono previste, in particolare, le seguenti classi di rischio:
  - "*Residual Risk*", in cui rientrano tutti i clienti ordinari;
  - "*Low Risk*", in cui rientrano i clienti che presentano alcuni fattori di rischio;
  - "*Medium Risk*", in cui rientrano i clienti che presentano più fattori di rischio;
  - "*High Risk*", in cui rientrano i clienti che presentano c.d. "rischi superiori" ai sensi della normativa svizzera (tra questi, le relazioni bancarie con intermediari esteri in cui la Banca offre servizi di banca corrispondente; le relazioni riferite a conti transitori/ omnibus, le relazioni riferite a struttura complesse);
  - "PEP", in cui rientrano le persone politicamente esposte;
- ciascuna classe di rischio determina l'applicazione di specifici processi di *escalation* per l'apertura della relazione con il cliente, la revisione periodica dei dati e delle informazioni relative al cliente, un monitoraggio più approfondito delle operazioni e reporting interno. Tali processi sono più o meno articolati a seconda del livello di esposizione al rischio di riciclaggio e finanziamento del terrorismo;
- la modifica della classe di rischio di un cliente in corso di rapporto (in particolare, il *downgrade* della classe di rischio) è soggetta a una specifica procedura autorizzativa che coinvolge la funzione Compliance;
- le modifiche della classe di rischio in corso di rapporto contrattuale devono essere specificamente motivate e documentate;

- sono previsti controlli periodici e automatici sui fattori di rischio che interessano i clienti al fine di identificare eventuali discrepanze rispetto ai dati effettivi della relazione bancaria che potrebbero richiedere un aggiornamento del profilo di rischio (c.d. "*Risk Hits*").

Infine, la Norma AML dispone che in relazione a ciascun nuovo rapporto contrattuale sia effettuato un processo di *due diligence*, ossia di analisi (1) delle ragioni e dello scopo della relazione bancaria, (2) dell'origine degli averi che il cliente intende conferire alla banca per l'apertura della relazione (3) della struttura del rapporto nonché (4) del *background* di ciascun cliente, in quanto soggetto che origina ricchezza in favore dell'avente diritto economico (ciò al fine di conoscere l'origine e la destinazione dei fondi oggetto di trasferimento sui conti della Banca).

Con specifico riferimento al suddetto processo di *due diligence*, la Norma AML e la Norma Operativa 2.1. Procedura Apertura Rapporti d'Affari prevedono i seguenti presidi e controlli:

- prima dell'apertura di ciascuna relazione il Relationship Manager è tenuto a raccogliere dal cliente, tramite la compilazione di apposito Profilo KYC e la richiesta di documentazione di base obbligatoria, i dati e le informazioni necessarie all'identificazione e alla classificazione dello stesso nell'ambito delle categorie di rischio;
- con specifico riferimento ai clienti classificati nelle categorie "High Risk" e PEP, è prevista l'applicazione di misure rafforzate di *due diligence*, specificamente disciplinate nelle Norme Operative. In particolare:
  - le misure rafforzate di due diligence relative ai clienti PEP sono disciplinate dalla Norma Operativa 2.30 Procedura Relazioni PEP;
  - le misure rafforzate relative ai conti collettivi e transitori nonché ai conti correnti e depositi rubricati su relazioni esistenti e riferibili ad Aventi Diritto Economico diversi da quelli precedentemente indicati sono disciplinati dalla Norma Operativa 2.42 "Conti Collettivi / Conti Transitori";
  - le misure rafforzate relative alle operazioni per cassa, dettagliate nella Norma Operativa 2.45 "*Prelevamenti e Versamenti per cassa*".
- sono previsti specifici processi di due diligence fiscale, al fine di evitare il coinvolgimento della Banca nella commissione di un delitto fiscale qualificato o, in relazione alle relazioni cross-border, nella contravvenzione di disposizioni fiscali applicabili nei paesi di residenza della clientela (cfr. Norma Operativa 2.55 "*Conformità fiscale delle relazioni bancarie*");
- sono previsti processi di registrazione e monitoraggio della documentazione mancante, scaduta o soggetta a rinnovo nonché specifici processi di attivazione delle funzioni competenti per il recupero dei documenti sospesi basati sulla relativa rilevanza ai fini dell'apertura del rapporto. In particolare, sono previste misure di blocco delle relazioni bancarie a seconda della rilevanza della documentazione e dei ritardi nella raccolta della documentazione mancante;
- è prevista l'interruzione della relazione d'affari qualora la Banca accerti il rilascio di informazioni false in merito all'identificazione del cliente o al detentore del controllo o all'Avente Diritto Economico, nonché in presenza di criticità nell'adempimento degli obblighi AML riferiti alla specifica relazione d'affari che potrebbero raccomandare la cessazione del rapporto contrattuale con il cliente;

L'apertura di ciascuna relazione è soggetta ad uno specifico processo di approvazione che prevede diversi livelli di *escalation* a seconda della classe di rischio cui appartiene il cliente e in casi di maggior rischio il coinvolgimento della funzione L&C e del Comitato Accettazione Clienti.

d) Revisione periodica dei rapporti con la clientela e monitoraggio delle transazioni

La Norma AML prevede specifici processi di monitoraggio costante dei dati relativi alla clientela, nonché delle operazioni dalla medesima poste in essere.

In particolare:

- la Banca ha adottato sistemi informatici per il monitoraggio costante di tutte le transazioni attinenti alle relazioni d'affari aperte dai clienti presso la Banca stessa;
- è previsto un sistema automatico di rilevazione delle operazioni considerate "*a rischio superiore*" c.d. "AML HITS", basato su fattori di rischio predeterminati;
- il processo di rilevazione automatico delle AML HITS non esclude la possibilità di rilevare e trattare con diligenza eventuali "*transazioni inconsuete 3333o inusuali*" non rilevate dai sistemi informatici in quanto solo prospettate o annunciate dal cliente;
- sono previsti processi specifici di analisi ed evasione delle AML Hits da parte della funzione L&C che prevedono controlli e reporting periodici di secondo livello verso il CRO, i Capi Divisione e il CORI nonché specifici processi di escalation a vari livelli, che nei casi più gravi coinvolgono anche il CRO e il CAC;
- sono previsti degli screening automatici e periodici dei clienti registrati, nonché dei soggetti ordinanti e dei beneficiari di bonifici in entrata e in uscita rispetto alle *black lists* emesse dalle autorità nazionali e internazionali competenti (in particolare è previsto l'utilizzo di Worldcheck e la predisposizione di una specifica *Black List* PKB);

I suddetti processi di monitoraggio dei dati e delle informazioni riferibili alla clientela avvengono a diversi livelli di controllo: (a) i controlli di primo livello vengono effettuati dai Relationship Manager nell'ambito delle attività di ordinaria gestione della clientela, nonché dai Capi Mercato, dai Capi Team e dai responsabili delle Divisioni 1 e 2; (b) i controlli di secondo livello vengono effettuati dalla funzione Compliance, alla quale è richiesto di assicurare che i sistemi di monitoraggio della clientela siano conformi alla normativa interna e alle disposizioni normative e regolamentari locali nonché presidiare le attività condotte dalla prima linea e dalla clientela stessa sulle relazioni d'affari.

Le attività di monitoraggio possono determinare la variazione della classe di appartenenza di ciascun cliente e l'aggiornamento del relativo profilo. Tali variazioni sono sottoposte a specifici processi autorizzativi, in cui è sempre coinvolta la funzione L&C.

Qualora a seguito delle operazioni di monitoraggio vengano individuate operazioni a rischio di riciclaggio, sono previste procedure di analisi delle stesse che, nei casi più gravi possono portare al blocco della relazione bancaria o alla segnalazione della stessa alle autorità competenti. In particolare, l'accettazione di fondi in entrata è disciplinata da una specifica Norma Operativa che prevede la richiesta di approfondimenti sull'operazione disposta e nei casi più gravi il ritorno alla banca ordinante di tutti i fondi in entrata per i quali le istruzioni di accredito non siano conformi alla normativa interna (Norma Operativa 5.36 Fondi in Entrata).

e) Obblighi di reporting e segnalazione

La Norma AML prevede l'obbligo in capo ai Dipendenti rilevanti di comunicare alla funzione L&C:

- qualsiasi operazione che sia stata rifiutata a causa di manifesto e fondato sospetto di riciclaggio o di collegamento ad una organizzazione criminale;

- qualsiasi operazione per la quale si abbia il fondato sospetto che il cliente faccia capo ad una organizzazione criminale oppure che i relativi patrimoni siano dell'organizzazione stessa;
- il rifiuto da parte del cliente a collaborare agli accertamenti richiesti dalla Banca.

E' previsto in capo alla funzione L&C l'obbligo di analizzare tutte le operazioni sospette di riciclaggio e di comunicarle, su delega della Direzione Generale, alle autorità competenti, secondo i moduli e le procedure messe a disposizione della autorità di vigilanza. Le relazioni oggetto di segnalazione al MROS, a seconda dei casi, possono essere bloccate dalla funzione L&C: è previsto in ogni caso il blocco delle relazioni oggetto di segnalazione ex art 9 cpv let.c) della "*Legge federale relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo*".

La funzione L&C è tenuta a tenere traccia di tutte le segnalazioni effettuate nonché a motivare e documentare specificamente eventuali casi per i quali abbia deciso di non procedere alla segnalazione stessa.

La funzione L&C informa:

- il CRO e il responsabile di Divisione 1 o 2 (a seconda di chi sia responsabile del cliente) in merito ad ogni segnalazione effettuata al MROS;
- il CAC in merito alle relazioni segnalate al MROS che (1) non siano state successivamente inoltrate alle competenti autorità di perseguimento penale; (2) siano state inoltrate a tali autorità ma siano state abbandonate o per le quali sia stato disposto il non luogo a procedere. Ciò affinché il CAC possa deliberare in merito al prosieguo o alla chiusura della relazione d'affari;
- il CORI in merito alle segnalazioni che comportano rischi reputazionali rilevanti.

f) Presidi aggiuntivi relativi ai trasferimenti /accettazione di fondi/ valori per cassa

La Banca ha adottato una specifica Norma Operativa (Cfr. la Norma Operativa n. 2.45 "*Prelevamenti e Versamenti per cassa*") che disciplina la gestione di 1) prelevamenti e versamenti di denaro contante e 2) "*operazioni di cassa*", intendendosi per queste, ai sensi dell'art. 2 b dell' Ordinanza FINMA sul riciclaggio di denaro e il finanziamento del terrorismo del 03 giugno 2015, "*ogni operazione in contanti, in particolare il cambio, l'acquisto e la vendita di metalli preziosi, la vendita di assegni di viaggio, la sottoscrizione di titoli al portatore, obbligazioni di cassa e prestiti obbligazionari, l'incasso in contanti di assegni, sempre che queste operazioni non siano legate a una relazione d'affari continua*".

Con riferimento ai prelevamenti e versamenti di denaro contante, in linea di principio la Banca non è favorevole all'esecuzione di operazioni di importi rilevanti e scoraggia i propri clienti dall'effettuarle, invitandoli ad operare tramite bonifici bancari.

Nei casi in cui i clienti decidano di procedere all'esecuzione di prelevamenti e versamenti in contanti, la Banca pone in essere le seguenti limitazioni operative:

1) per ogni transazione singola di importo pari o superiore a CHF 50.000 è richiesta l'autorizzazione del consulente e del capo team;
2) per le transazioni cumulate nel corso dell'anno solare di importo pari o superiore a CHF 200.000 è richiesta l'autorizzazione del consulente e del capo team;

I processi autorizzativi sono peraltro basati sul principio di diligenza accresciuta, secondo cui il consulente alla clientela è tenuto ad osservare criteri di diligenza accresciuta nell'accertamento del retroscena economico dell'operazione, tramite richiesta di chiarimenti al cliente e raccolta di documentazione a supporto. Tali operazioni sono autorizzate previa valutazione - sulla base dei

chiarimenti forniti dal cliente e della documentazione raccolta - della plausibilità dell'operazione economica.

I risultati dei chiarimenti sono documentati e registrati, così come le altre transazioni soggette a verifica, nei sistemi informatici adottati dalla Banca ai fini dell'antiriciclaggio.

La Banca ha inoltre adottato degli strumenti di controllo sulle movimentazioni in contanti.

Quanto alle "*operazioni di cassa*", trattasi di operazioni marginali, in quanto effettuate in via eccezionale e solo per ordine di clienti della Banca. Non sono effettuate su ordine di soggetti che, non avendo relazioni aperte con la Banca, non sono clienti della stessa.

Anche le "*operazioni di cassa*" sono soggette a specifici limiti operativi, in particolare:

1) non possono essere effettuate per importi superiori a CHF 25.000
2) per "*operazioni di cassa*" superiori a CHF 10'000 è richiesta l'autorizzazione preventiva del consulente.

g) Presidi relativi all'accettazione e consegna di averi fisici (ad esempio, contante, titoli fisici, metalli preziosi e carte valori)

L'attività di custodia di valori fisici e di locazione di cassette di sicurezza è svolta dalla Banca in misura marginale, su specifica richiesta da parte dei clienti. Ciò nonostante, la Banca ha adottato specifiche Norme Operative (Cfr. Norma Operativa 5.52 "*Valori fisici in custodia presso PKB*", Norma Operativa e Norma Operativa 5.12 "*cassette di sicurezza*") che disciplinano i presidi adottati in relazione alla gestione di averi fisici depositati dai clienti presso la Banca e alle quali si rinvia ai fini della prevenzione dei reati oggetto della presente Parte Speciale.

Con specifico riferimento agli averi fisici depositati dalla clientela in cassette di sicurezza, si precisa – ai fini dell'ipotetica configurazione dei reati oggetto della presente Parte Speciale - che la Banca, come previsto dalla normativa svizzera applicabile, non viene conoscenza dei beni ivi depositati dal cliente, salvo che siano notificati ordini di sequestro da parte della Procura Pubblica svizzera.

8. Reati tributari (art. 25-quinquiesdecies, D.Lgs., 8 giugno 2001, n. 231)

In base al quadro legale di riferimento italiano, l'art. 39, comma 2, del D.L. 26 ottobre 2019, n. 124 (convertito con modificazioni dalla L. 19 dicembre 2019, n. 157), mediante l'introduzione all'interno del D.Lgs. n. 231/2001 dell'art. 25-*quinquiesdecies*, ha esteso l'ambito applicativo della responsabilità degli enti per illeciti amministrativi dipendenti da reato anche ad alcune ipotesi, tassativamente individuate, di fattispecie delittuose di cui al D.Lgs., 10, marzo 2000, n. 74. (i.e. quelle di cui agli artt. 2; 3; 8; 10 e 11). In maggiore dettaglio, l'art. 25-*quinquiesdecies,* del D.Lgs. n. 231/2001 annovera tra i c.d. "reati presupposto" della responsabilità degli enti per illeciti amministrativi dipendenti da reato i seguenti reati tributari:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, D.Lgs. 74/2000);
- dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000);
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.Lgs. 74/2000);
- occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000);
- sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000).

Il catalogo dei c.d. "reati tributari" che possono assurgere a reati presupposto della responsabilità degli enti per illeciti amministrativi dipendenti da reato è stato, poi, ulteriormente ampliato per effetto dell'emanazione del D.Lgs., 14 luglio 2020, n. 75, a mezzo del quale è stata recepita nell'ordinamento italiano la Direttiva (UE) n. 2017/1371 (c.d. "Direttiva PIF") relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale.

In particolare, l'art. 5, comma 1, lett. c), D.Lgs. n. 75/2020 ha inserito all'interno dell'art. 25-*quinquiesdecies,* del D.Lgs. n. 231/2001 il comma 1-*bis*, ai sensi del quale possono costituire reati presupposto ai fini della disciplina di cui al D.Lgs. n. 231/2001 anche le seguenti fattispecie delittuose:

- dichiarazione infedele (art. 4 D.Lgs. 74/2000);
- omessa dichiarazione (art. 5 D.Lgs. 74/2000);
- indebita compensazione (art. 10-*quater* D.lgs. 74/2000);

e ciò, a condizione che i predetti reati tributari siano stati commessi "*nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*". Per completezza, si rappresenta che, per effetto di una modifica apportata dall'art. 2, D.Lgs. n. 75/2020 all'art. 6, D.Lgs. n. 74/2000, le fattispecie delittuose di cui agli art. 2, 3 e 4 del D.Lgs. n. 74/2000 sono oggi punibili anche a titolo di tentativo (e come tali suscettibili di assumere rilevanza anche ai fini della configurabilità della responsabilità degli enti per illeciti amministrativi dipendenti da reato), laddove gli atti diretti in modo non equivoco a commettere uno dei reati tributari di cui alle predette disposizioni normative siano stati "*compiuti anche nel territorio di altro Stato membro dell'Unione europea, al fine di evadere l'imposta sul valore aggiunto per un valore complessivo non inferiore a dieci milioni di euro*".

Si provvede ad illustrare qui di seguito le caratteristiche che contraddistinguono ciascuna fattispecie di reato tributario annoverata tra i c.d. reati presupposto ("di seguito i "**Reati Tributari Presupposto**").

8.1. Reati Tributari Presupposto

8.1.1. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, D.Lgs. n. 74/2000)

Commette il reato in oggetto chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto (dolo specifico), avvalendosi di fatture o altri documenti per operazioni inesistenti[8], indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

In particolare, si evidenzia che ai fini della configurazione della fattispecie delittuosa in parola non è richiesto il superamento di alcuna soglia quantitativa di punibilità.

In particolare, il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti allorché tali fatture o documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti ai fini di prova nei confronti dell'Amministrazione finanziaria.

Per completezza, si rappresenta che, il soggetto che ha commesso il reato di "*Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti*", in deroga alle regole generali di cui all'art. 110 del c.p., non può essere chiamato a rispondere a titolo di concorso nel reato di "*emissione di fatture o altri documenti per operazioni inesistenti*" di cui all'art. 8, D.Lgs. n. 74/2000 commesso da un soggetto terzo che ha emesso le fatture o altri documenti per operazioni inesistenti (cfr. Sezione 8.1.3 sotto).

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

Commette il reato in oggetto chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente[9], oppure avvalendosi di documenti falsi – diversi da quelli rilevanti ai fini della configurabilità della fattispecie delittuosa di cui all'art. 2, D.Lgs. n. 74/2000 – o di altri mezzi fraudolenti[10] idonei a ostacolare l'attività accertativa dell'Amministrazione finanziaria o a indurre la stessa in errore, indica in una delle dichiarazioni relative a dette imposte (imposte dirette e IVA) elementi attivi[11] per un ammontare inferiore a quello effettivo, oppure elementi passivi, crediti o ritenute fittizi.

Perché possa considerarsi integrata la fattispecie delittuosa in parola è richiesto il superamento di una duplice soglia di punibilità. In particolare, a tal fine è necessario che:

- l'imposta evasa, per effetto della condotta descritta dalla norma in esame, sia superiore, con riferimento alle singole imposte, a Euro 30.000; e

---

[8] Per quanto attiene alla nozione di "*fatture o altri documenti per operazioni inesistenti*", ai sensi dell'art. 1, comma 1, lett. a), del D.Lgs. n. 74/2000, si considerano tali le fatture o gli altri documenti aventi analoga rilevanza probatoria che si caratterizzano per il fatto di essere emessi a fronte di "*operazioni non realmente effettuate in tutto o in parte o che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale*" (inesistenza oggettiva), oppure che "*riferiscono l'operazione a soggetti diversi da quelli effettivi*" (inesistenza soggettiva).

[9] Per quanto attiene alla nozione di "*operazioni simulate oggettivamente o soggettivamente*", ai sensi dell'art. 1, comma 1, lett. g-*bis*), D.Lgs. n. 74/2000 si considerano tali le operazioni "*apparenti*", ossia le operazioni "*poste in essere con la volontà di non realizzarle in tutto o in parte*" (simulazione assoluta), oppure le operazioni "*riferite a soggetti fittiziamente interposti*".

[10] Ai sensi dell'art. 1, comma 1, lett. g-*ter*), D.Lgs. n. 74/2000, si considerano " "*mezzi fraudolenti"…le condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determina una falsa rappresentazione della realtà*". Tuttavia, come stabilito dal terzo comma dell'art. 3, D.Lgs. n. 74/2000, non costituiscono, invece, "*mezzi fraudolenti*" ai fini del primo comma del predetto art. 3, "*…la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali*".

[11] Vale a dire, ai sensi dell'art. 1, comma 1, lett. b), D.Lgs. n. 74/2000, quelli che concorrono "*in senso positivo* …" alla determinazione del reddito, della base imponibile o dell'imposta dovuta.

- l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, sia superiore: **(i)** al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o comunque a Euro 1,5 milioni; oppure **(ii)** l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta sia superiore al 5% dell'ammontare dell'imposta medesima o comunque a Euro 30.000.

Ai sensi, dell'art. 3, comma 2, D.Lgs. n. 74/2000 il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti ai fini di prova nei confronti dell'Amministrazione finanziaria.

Da ultimo, si rileva che non assumono rilevanza ai fini della configurabilità della fattispecie delittuosa in esame, la mera violazione degli obblighi di fatturazione e di annotazione di elementi attivi nelle scritture contabili obbligatorie, o l'indicazione nelle fatture o nelle annotazioni nelle scritture contabili obbligatorie di elementi attivi inferiori a quelli reali.

8.1.3. Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.Lgs. n. 74/2000)

Commette il reato in oggetto chiunque, al fine di consentire a soggetti terzi di evadere le imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti ([12]).

Il soggetto che emette fatture o altri documenti per operazioni inesistenti, oppure colui che partecipa alla commissione del reato di cui alla norma in esame, in deroga alle regole generali di cui all'art. 110 del c.p. non è punibile anche a titolo di concorso nel reato di "*Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti*" di cui all'art. 2, D.Lgs. n. 74/2000 commesso dal terzo che si avvale di tali documenti, così pure tale terzo non è punibile anche a titolo di concorso nel reato di emissione in oggetto.

8.1.4. Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. n. 74/2000)

L'art. 10, D.Lgs. n. 74/2000 prevede che, "*salvo che il fatto costituisca più grave reato*", è punito chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, oppure di consentire a terzi di evadere le predette imposte, distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, così da precludere agli organi preposti all'attività di accertamento la possibilità di procedere alla "*ricostruzione dei redditi o volume di affari*".

8.1.5. Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. n. 74/2000)

Commette il reato in oggetto chiunque, al fine di sottrarsi al pagamento delle imposte sui redditi o sul valore aggiunto, oppure di interessi o sanzioni amministrative tributarie per un importo superiore a Euro 50.000 (soglia di punibilità), pone in essere, sui beni propri o di terzi, atti dispositivi simulati o altri atti connotati da fraudolenza, idonei a rendere in tutto o in parte inefficaci le procedure riscossione coattiva finalizzate al soddisfacimento del credito erariale.

Commette il reato in oggetto, inoltre, chiunque, nell'ambito di una procedura di c.d. "transazione fiscale" di cui all'art. 182-*ter*, R.D., 16 marzo 1942, n. 267, al fine di ottenere per sé o per altri un minor pagamento di tributi e accessori, indica nella documentazione presentata elementi attivi inferiori a quelli reali o elementi passivi fittizi per un ammontare complessivo superiore a Euro 50.000.

[12] Per la definizione di "operazione inesistente" cfr. art. 1, comma 1, lett. a), D.Lgs. n. 74/2000.

8.1.6. Dichiarazione infedele (art. 4, D.Lgs. n. 74/2000)

La fattispecie di reato in oggetto, in linea generale, si configura, salvo che non ricorrano i presupposti per ritenere integrate le più gravi fattispecie delittuose di cui agli artt. 2 e 3, D.Lgs. n. 74/2000, allorché un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative alle predette imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti. Perché si possa ritenere integrata la fattispecie delittuosa in esame è necessario, sempre in linea generale, il superamento di una duplice soglia di punibilità. E, infatti, richiesto che:

- l'imposta evasa sia superiore, con riferimento alle singole imposte, a Euro 100.000; e
- l'ammontare complessivo degli elementi attivi sottratti a imposizione, anche per effetto dell'indicazione in dichiarazione di elementi passivi inesistenti, sia superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o, in ogni caso, a Euro 2 milioni.

Ai fini della configurazione del reato di dichiarazione infedele non si tiene conto della non corretta classificazione e valutazione di elementi attivi o passivi oggettivamente esistenti, con riferimento ai quali i criteri di classificazione e valutazione concretamente adottati sono stati indicati in bilancio o in altri documenti aventi rilevanza ai fini fiscali, nonché, della violazione di principi di competenza, inerenza o dell'indeducibilità di elementi passivi reali.

Non danno luogo a fattispecie aventi rilevanza penale le valutazioni che complessivamente considerate differiscono da quelle corrette in misura inferiore al 10%.

Ciò posto, il reato tributario in parola rileva come Reato Tributario Presupposto esclusivamente nell'ipotesi in cui sia stato commesso "*nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*".

8.1.7. Omessa dichiarazione (art. 5, D.Lgs. n. 74/2000)

La fattispecie di reato in oggetto, in linea generale, si configura, allorché un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, pur essendo gravato da uno specifico obbligo in tal senso, una delle dichiarazioni relative alle predette imposte.

Al fine di ritenere integrata la fattispecie delittuosa in esame è necessario, sempre in linea generale, il superamento di una duplice soglia di punibilità. Ed infatti, è richiesto che l'imposta evasa risulti essere superiore, con riferimento a ciascuna imposta considerata dalla norma, a Euro 50.000.

Ha rilevanza penale anche alla condotta del soggetto che omette, pur essendovi obbligato, di presentare la dichiarazione di sostituto di imposta; e ciò a condizione che l'ammontare delle ritenute non versate ecceda l'importo di Euro 50.000 (soglia di punibilità).

Ciò posto, il reato tributario in parola rileva come Reato Tributario Presupposto esclusivamente nell'ipotesi in cui sia stato commesso "*nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*".

8.1.8. Indebita compensazione (art. 10-quater, D.Lgs. n. 74/2000)

In linea generale, risponde del reato di indebita compensazione chi "*non versa le somme dovute*[13]" utilizzando in compensazione crediti non spettanti (o inesistenti) per un importo annuo superiore a Euro 50.000.

Ciò posto, il reato tributario in parola rileva come Reato Tributario Presupposto esclusivamente nell'ipotesi in cui sia stato commesso "*nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*".

8.2. Attività aziendali sensibili

Il rischio di commissione dei Reati Tributari Presupposto ai sensi della normativa legale italiana, può presentarsi, in linea di principio, in diverse attività aziendali.

Per quanto riguarda la posizione della Banca quale soggetto passivo di imposte e tasse previste dall'ordinamento tributario italiano, laddove applicabili, l'attività sensibile - identificata dal Modello come quella la cui effettuazione presenta il maggior rischio che siano posti in essere i comportamenti illeciti come sopra descritti – è l'attività transfrontaliera verso la clientela – attuale o potenziale – residente in Italia (o tenuta ad obblighi fiscali in Italia).

Le ulteriori attività aziendali sensibili ai reati in parola sono quelle che, in ogni caso, presentano profili di collegamento con soggetti residenti ai fini fiscali in Italia o comunque tenuti all'adempimento di obblighi tributari in Italia, nonché quelle che possono dare luogo ad ipotesi di concorso della Banca in condotte illecite poste in essere da tali soggetti, come:

- l'instaurazione e gestione dei rapporti con la clientela e la gestione dei relativi flussi finanziari;
- l'acquisto, gestione e cessione di partecipazioni societarie, titoli e altri strumenti finanziari;
- l'acquisizione di beni e servizi e l'assegnazione di incarichi professionali;
- la gestione di omaggi, spese di rappresentanza e pubblicità.

I comitati e le unità organizzative della Banca principalmente coinvolte nelle attività sensibili sono le seguenti:

- Audit & Risk Committee ("ARC");
- Direzione Generale ("DG");
- Divisione Private Banking;
- Divisione Finance & Markets;
- Divisione Risk Management, Compliance, Controlli e Credit Office.

8.3. Presìdi procedurali e di controllo

a). Premessa

Si riportano di seguito i presìdi procedurali e di controllo adotti dalla Banca volti alla rilevazione, misurazione, gestione e controllo del rischio fiscale con particolare riferimento all'operatività della

[13] Sul punto, si rileva che l'Amministrazione finanziaria nella Circolare n. 28/E del 4 agosto 2006 si è espressa nel senso di ritenere che ai fini della configurazione della fattispecie delittuosa in parola rileva l'omesso versamento di qualunque debito di imposta e non solo di quelli aventi ad oggetto le imposte dirette e l'IVA.

Banca stessa nei confronti di soggetti residenti ai fini fiscali in Italia o comunque tenuti all'adempimento di obblighi tributari in Italia.

I presìdi procedurali e di controllo riportati nella presente Sezione di Parte Speciale assumono altresì rilevanza al fine della prevenzione dei reati di Riciclaggio e Autoriciclaggio (cfr. Sezione 7 della Parte Speciale del Modello)

Con riferimento alla variabile fiscale, la Banca ha definito i propri obiettivi e la propria propensione al rischio fiscale all'interno del Risk Appetite Framework di Gruppo, ove si afferma che:

- non vi è alcuna propensione al rischio di non conformità alle norme applicabili nei confronti della Banca e dei suoi collaboratori, incluse quelle rilevanti ai fini dell'attività cross-border;
- la Banca instaura relazioni con clientela che rispetta la normativa fiscale applicabile ("Tax compliance") e limita le relazioni con clientela che potrebbero comportare un rischio accresciuto. La clientela è sottoposta ad un processo di accettazione che comporta una valutazione preventiva e una rivalutazione periodica della clientela esistente.

b). Presìdi procedurali e di controllo

La Banca promuove e mantiene – all'interno della propria *risk governance* – un adeguato sistema di controllo interno a presidio del rischio fiscale, volto a consentire una conduzione dell'attività della Banca tale da minimizzare il rischio di operare (o concorrere ad operare) in violazione di norme di natura tributaria, o in contrasto con i princìpi o con le finalità dell'ordinamento tributario.

I principali processi aziendali oggetto di monitoraggio sono rappresentati da:

- svolgimento di attività transfrontaliera verso la clientela – attuale o potenziale – residente in Italia (o tenuta ad obblighi fiscali in Italia);
- corretta rilevazione e rappresentazione dell'operatività della Banca nei propri sistemi contabili e gestionali;
- predisposizione delle dichiarazioni fiscali, liquidazione e versamento delle imposte e tasse dovute;
- instaurazione e gestione dei rapporti con la clientela e gestione dei relativi flussi finanziari;
- acquisto, gestione e cessione di partecipazioni societarie, titoli e altri strumenti finanziari;
- acquisizione di beni e servizi e assegnazione di incarichi professionali;
- gestione di omaggi, spese di rappresentanza e pubblicità.

La concreta effettuazione delle attività di monitoraggio e controllo del rischio fiscale nei confronti dell'Italia è disciplinata da uno specifico *framework* normativo interno volto a regolamentare i processi, i ruoli e le responsabilità, comprensivo, oltre che della Norma Operativa. 2.50 recante "*IT) Attività transfrontaliera (cross-border) MANUALE PAESE "ITALIA"*", dei seguenti documenti concernenti le suddette aree di attività:

- "*Regolamento di Amministrazione e Gestione*" (RAG) e Norma Operativa. 5.14 recante "*Tasse/imposte, in generale*", per quel che concerne la gestione degli obblighi fiscali della Banca;
- si rinvia ai presidi procedurali riportati nella Sezione di Parte Speciale relativa ai reati di "*Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e autoriciclaggio (art. 25-octies) e reati con finalità di terrorismo o di eversione dell'ordine*

democratico (art. 25 quater)" (cfr. Sezione 7 della Parte Speciale del Modello), per quel che concerne il contrasto al riciclaggio di denaro e al finanziamento del terrorismo;

- Norma Operativa 2.55 recante "*Conformità fiscale delle relazioni bancarie*" e Norma Operativa 2.59 recante "*Scambio Automatico di Informazioni*", per quel che concerne la gestione della conformità fiscale della clientela;
- Norma Operativa 2.32 recante "*Operatività con società fiduciarie italiane*", per quel che concerne la gestione del rischio fiscale relativo a prodotti e servizi offerti alla clientela italiana;
- Norma Operativa 5.71 recante "*Fondi d'investimento di private equity o investimenti assimilabili*", per quel che concerne l'acquisto, gestione e cessione di partecipazioni societarie, titoli e altri strumenti finanziari;
- Norma Operativa 12.2 recante "*Norma operativa in materia di procurement*" per quel che concerne acquisto, gestione e cessione di partecipazioni societarie, titoli e altri strumenti finanziari; si rinvia inoltre ai presidi procedurali riportati nella Sezione di Parte Speciale relativa ai reati contro la Pubblica Amministrazione (cfr. Sezione 1 della Parte Speciale del presente Modello);
- si rinvia ai presidi procedurali riportati nella Sezione di Parte Speciale relativa ai reati contro la Pubblica Amministrazione (cfr. Sezione 1.3 lett. c) della Parte Speciale) per quel che concerne gestione di omaggi, spese di rappresentanza e pubblicità;
- sono state infine definite delle procedure per la gestione del rischio fiscale, come in allegato al Manuale Italia.

Gli elementi fondamentali sui quali si basa il sistema di controllo del rischio fiscale sono i seguenti:

- definizione ed individuazione dei soggetti responsabili/autorizzati, in base al relativo ruolo, a porre in essere attività e processi;
- separazione delle attività tra chi autorizza, chi esegue e chi controlla. Tale segregazione è garantita dall'intervento nei processi di gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari di più soggetti al fine di garantire indipendenza e obiettività dei processi;
- effettuazione di:
  - in applicazione delle norme sullo scambio automatico delle informazioni, controlli sulla completezza ed accuratezza delle informazioni relative alla situazione fiscale dei rapporti con la clientela e delle informazioni da trasmettere alle autorità fiscali;
  - controlli sulla conformità alla normativa tributaria di riferimento dei prodotti e servizi offerti alla clientela (ad esempio, verifica periodica dell'esistenza di *hallmarks*, ossia indici di rischio di elusione o evasione fiscale ai sensi della Direttiva 2018/822/UE (DAC 6));
  - controlli sulla corretta emissione delle fatture attive e della 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, nonché sulla coerenza con il rapporto sottostante dei dati del soggetto destinatario del relativo pagamento e della localizzazione del relativo conto;
  - controlli sulla correttezza delle dichiarazioni periodiche, della liquidazione di imposte e tasse e dei relativi versamenti;

- tracciabilità del processo, consistente nell'adeguata documentazione delle diverse attività svolte e nella possibilità di poter verificare *ex post*, anche tramite appositi supporti documentali, il processo di decisione, autorizzazione e svolgimento delle stesse.

Inoltre, la gestione e mitigazione del rischio fiscale è effettuata nell'ambito del Sistema di Controllo Interno (cfr. Sezione 2.7.2 della Parte Generale del Modello).

c). Principi di comportamento

Le unità organizzative della Banca, a qualsiasi titolo coinvolte nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari oggetto del protocollo, come pure tutti i dipendenti, sono tenuti nei rispettivi ambiti a:

- garantire la corretta e veritiera rappresentazione dell'operatività e dei risultati della Banca nelle dichiarazioni fiscali;
- eseguire correttamente e tempestivamente gli adempimenti fiscali richiesti dalla normativa applicabile;
- mantenere, nel rispetto della normativa applicabile, un rapporto collaborativo e trasparente con le Autorità fiscali italiane;
- evitare (o comunque essere parte di) forme di pianificazione fiscale che possano essere giudicate aggressive da parte delle Autorità fiscali italiane;
- evitare di proporre alla clientela prodotti e servizi che consentano di conseguire indebiti vantaggi fiscali non altrimenti ottenibili, avendo altresì cura di evitare il coinvolgimento della Banca in operazioni fiscalmente irregolari poste in essere dalla clientela stessa;
- rispettare le diposizioni atte a garantire idonei prezzi di trasferimento per le operazioni infragruppo.

In ogni caso è fatto divieto di porre in essere/collaborare alla realizzazione di comportamenti che possano rientrare nelle fattispecie di Reati Tributari Presupposto ai fini del D. Lgs. n. 231/2001, come, a titolo meramente esemplificativo e non esaustivo:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre in errore le Autorità fiscali italiane;
- pagare 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, nonché la coerenza con il sottostante accordo contrattuale;
- emettere fatture o rilasciare altri documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- impiegare strutture o entità societarie artificiose, non correlate all'attività imprenditoriale, all'unico scopo di eludere la normativa fiscale.

9. Delitti in materia di strumenti di pagamento diversi dai contanti

9.1. Premessa

Il D.Lgs. 184/2021, nel dare attuazione alla Direttiva 2019/713/UE, ha introdotto nel D.Lgs. 231/2001 l'art. 25-octies.1 nel quale vengono inseriti tra i reati presupposto alcune fattispecie a tutela degli "*strumenti di pagamento*", come meglio descritte nel Par. 1.1. del presente Capitolo di Parte Speciale.

Ai fini della presente Parte Speciale, si applicano le seguenti definizioni previste dall'art. 1 dello stesso D.Lgs. 184/2021:

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

b. per "*dispositivo, oggetto o record protetto*" si intende *"un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta, per esempio mediante disegno, codice o firma*";

c. per "*mezzo di scambio digitale*" indica "*qualsiasi moneta elettronica" e la "valuta virtuale".*

In particolare,

i. per *"moneta elettronica"* si intende ai sensi del dell'art. 1, comma 2, lett. h ter), d.lgs. 385/1993 *"il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento come definite all'articolo 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11([14]), e che sia accettato da persone fisiche e giuridiche diverse dall'emittente".*

Non costituisce moneta elettronica:

- il valore monetario memorizzato sugli strumenti previsti dall'articolo 2, co. 2, lettera m), del D.Lgs. 11/2010 ([15])
- il valore monetario utilizzato per le operazioni di pagamento previste dall'articolo 2, comma 2, lettera n), del decreto legislativo 27 gennaio 2010, n. 11 ([16]).

([14]) L'attività, posta in essere dal pagatore o dal beneficiario, di versare, trasferire o prelevare fondi, indipendentemente da eventuali obblighi sottostanti tra pagatore e beneficiario.

([15]) Strumenti di pagamento utilizzabili solo in modo limitato, che soddisfino una delle seguenti condizioni: 1) strumenti che possono essere utilizzati per acquistare beni o servizi solo nei locali dell'emittente o all'interno di una rete limitata di prestatori di servizi vincolati da un accordo commerciale con l'emittente; 2) strumenti che possono essere utilizzati unicamente per l'acquisto di una gamma molto limitata di beni o servizi; 3) strumenti che sono regolamentati da un'autorità pubblica nazionale o regionale per specifici scopi sociali o fiscali, per l'acquisto di beni o servizi specifici da fornitori aventi un accordo commerciale con l'emittente e che hanno validità solamente in un unico Stato membro

([16]) Operazioni di pagamento effettuate da un fornitore di reti o servizi di comunicazione elettronica che, in aggiunta a detti servizi di comunicazione elettronica, consentono a un utente della rete o del servizio di effettuare operazioni di pagamento addebitandole alla relativa fattura o al conto pre-alimentato dell'utente stesso in essere presso il medesimo fornitore di reti o servizi di comunicazione elettronica, a condizione che il valore di ciascuna operazione di pagamento non superi euro 50 e il valore complessivo delle operazioni stesse non superi euro 300 mensili e che l'operazione di pagamento:

1) sia diretta all'acquisto di contenuti digitali e servizi a tecnologia vocale;
2) sia effettuata da o tramite un dispositivo elettronico nel quadro di un'attività di beneficenza, per effettuare erogazioni liberali destinate agli enti del terzo settore di cui all'articolo 4 del decreto legislativo 3 luglio 2017, n. 117, che esercitano in via esclusiva o prevalente una o più attività caritatevoli tra quelle di cui all'articolo 5 del decreto legislativo 3 luglio 2017, n. 117;
3) sia effettuata da o tramite un dispositivo elettronico per l'acquisto di biglietti relativi esclusivamente alla prestazione di servizi.

ii. Per "*valuta virtuale*", si intende, ai sensi dell'art. 1, co.1., lett. d) del D.Lgs. 184/2021 una "*rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente*".

Tali definizioni riprendono quelle proposte nella Direttiva 2019/71/UE.

9.2. Fattispecie delittuose

9.2.1. Indebito utilizzo e falsificazione di strumenti di pagamento (art. 493 ter c.p.)

L'art. 493 ter c.p. prevede tre ipotesi di reato.

La prima fattispecie di reato è costituita dall'indebito utilizzo di strumenti di pagamento. In particolare, commette il reato in oggetto chiunque indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti, al fine di trarne profitto per sé o per altri.

La seconda fattispecie, invece, consiste nella falsificazione o alterazione di strumenti di pagamento o di documenti analoghi che abilitino al prelievo di denaro contante o all'acquisto di beni o servizi;

La terza fattispecie di reato, infine, consiste nel possesso, cessione o acquisizione di strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. In quest'ultimo caso assume rilievo la provenienza illecita dello strumento di pagamento o degli altri documenti similari.

Al fine di considerare realizzato il reato non è necessario l'ottenimento di un profitto o il verificarsi di un danno, ossia non è necessario che la transazione giunga a buon fine.

9.2.2. Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater c.p.)

L'art. 493 quater c.p. punisce le condotte produzione, importazione, esportazione, vendita, trasporto, distribuzione, messa a disposizione, ottenimento per sé o per altri di apparecchiature, dispositivi o programmi informatici costruiti e progettati principalmente per commettere reati riguardanti strumenti di pagamento diversi dai contanti o specificamente adattati al medesimo scopo.

Il reato è punito a titolo di dolo specifico, richiedendo che le condotte siano poste in essere al fine di fare uso o di consentire ad altri l'uso delle apparecchiature e dei dispositivi sopraindicati nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti.

9.2.3. Frode nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640 ter c.p.)

L'art. 640 ter c.p. punisce chiunque alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. Nell'ambito dei reati in materia di strumenti di pagamento, l'art. 25 octies 1 del D.Lgs. 231/2001 introduce un'aggravante al reato di truffa informatica, consistente nella realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale.

La circostanza descritta può aver luogo attraverso l'accesso abusivo ai sistemi informatici dell'ente, la detenzione abusiva di codici di accesso, l'intercettazione di comunicazioni informatiche o telematiche.

9.2.4. Altri reati aventi ad oggetto strumenti di pagamento

Il D.Lgs. 231/2001 ricomprende tra i reati presupposto ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando abbia ad oggetto strumenti di pagamento diversi dai contanti.

Trattasi di una fattispecie residuale, che si applica qualora il fatto non integri un altro illecito amministrativo sanzionato più gravemente dal Decreto 231 stesso.

Le fattispecie richiamate sono molteplici e riguardano i seguenti Capi del Codice Penale italiano:

1) Titolo VII - Dei delitti contro la fede pubblica:

- Capo I - Della falsità in monete, in carte di pubblico credito e in valori di bollo;
- Capo II - Della falsità in sigilli o strumenti o segni di autenticazione, certificazione o riconoscimento;
- Capo III - Della falsità in atti;
- Capo IV - Della falsità personale

2) Titolo XIII – delitti contro il patrimonio:

- Capo I - Dei delitti contro il patrimonio mediante violenza alle cose o alle persone;
- Capo II - Dei delitti contro il patrimonio mediante frode.

9.3. Attività sensibili

Nell'ambito dell'attività della Banca il rischio che siano commessi reati attraverso strumenti di pagamento diversi dal contante risulta maggiormente elevato nelle seguenti attività:

a. gestione delle carte di credito aziendali;
b. emissione e rilascio di carte di credito/debito (in generale carte di pagamento) a favore dei clienti;
c. Gestione di sistemi di pagamento offerti alla clientela, diversi dalle carte di pagamento;
d. installazione e gestione di hardware e software (in particolare quelli relativi a sistemi di pagamento);
e. gestione e controllo degli accessi ai sistemi informatici

9.4. Principi comportamentali

È fatto divieto a tutti i destinatari del presente modello di:

- cedere e/o permettere l'utilizzo a terzi delle carte di credito aziendali messe a disposizione della Banca;
- utilizzare le carte di credito aziendali per motivi diversi da quelli consentiti;
- utilizzare impropriamente, falsificare o alterare strumenti di pagamento della clientela o della Banca (a titolo esemplificativo: carte di pagamento; applicazioni di e-banking; token di accesso all'e-banking);

- farsi rilasciare o prendere visione dei PIN delle carte di pagamento di cui non si è assegnatari o titolari (ad esempio aprendo le lettere indirizzate ai clienti contenenti le carte di pagamento e i PIN e rimuovendo i relativi sigilli, richiedendo o ottenendo in qualunque modo dai colleghi il PIN e i codici delle carte di pagamento ai medesimi assegnate);
- richiedere ai clienti o in qualsiasi modo ottenere le credenziali di accesso all'e-banking o i codici generati tramite token al fine di effettuare disposizioni di pagamento;
- utilizzare software o hardware o qualunque altro dispositivo idoneo ad alterare i sistemi informatici di pagamento della Banca;
- accedere ai sistemi informatici senza le necessarie autorizzazioni, al fine di alterare il sistema di pagamento della Banca.

9.5. Principi procedurali

L'attività di prevenzione dei reati oggetto del presente Sezione di Parte Speciale si basa su un sistema di presidi e misure di prevenzione disciplinate dalle Norme Operative adottate dalla Banca. In particolare, nella prevenzione dei reati in oggetto, la Banca ha adottato le seguenti Norme Operative:

- Norma operativa 2.11 "carte di credito" (incl. il paragrafo 2.11.5 Carte di credito corporate);
- Norma operativa 2.10 Carte Maestro
- Norma operativa 2.7. Accettazione di istruzioni della clientela (incl. i paragrafi 2.7.6.2 "ordini telefonici", 2.7.6.5 "e-mail");
- Norma operativa 11.1 "*gestione degli accessi applicativi*".
- Norma Operativa 11.12 "*Linee guida per la gestione dei rischi cibernetici*".

Di seguito si riportano i presidi che la Banca adotta in relazione alle diverse attività aziendali sensibili al fine di prevenire la commissione dei reati oggetto della presente Sezione di Parte Speciale.

a. *Gestione delle carte di credito aziendali*

La Banca ha adottato una norma operativa relativa al rilascio di carte di credito "*corporate*", ossia di carte di credito ad uso esclusivamente professionale, per il pagamento di beni e servizi a scopo professionale, inerenti il rapporto di lavoro con la Banca. Tale norma operativa definisce:

i. le modalità di emissione e dismissione delle carte di credito aziendali
ii. i soggetti autorizzati all'utilizzo delle carte di credito aziendali;
iii. i motivi e le modalità di utilizzo delle carte di credito aziendali.

Premesso che la Banca non emette direttamente carte di pagamento, ma ha stipulato con un istituto autorizzato al rilascio di moneta elettronica un accordo quadro per il rilascio di carte di credito a favore dei propri dipendenti, nell'ambito dei processi di emissione e dismissione delle stesse, la Banca ha adottato i seguenti presidi:

i. all'ufficio Payments & Cash è stato attribuito il compito di gestire i processi di rilascio e di dismissione delle carte di credito aziendali;
ii. il rilascio di carte di credito aziendali è subordinato alla presentazione da parte del dipendente all'ufficio Payments & Cash di un modulo, compilato e sottoscritto dal richiedente, dal responsabile diretto e dal Capo Divisione di riferimento (o dai relativi sostituti);

iii. l'ufficio Payments & Cash conserva in apposito dossier tutta la documentazione relativa alla richiesta, consegna e ritiro delle carte di credito di ciascun dipendente, nonché un registro delle carte di credito assegnate agli stessi;
iv. il registro delle carte di credito assegnate ai dipendenti, riporta per ciascun assegnatario i codici identificativi (ma non i PIN) e le date di richiesta, consegna, ritiro e scadenza delle carte di pagamento assegnate;
v. in caso di cessazione del rapporto di lavoro o collaborazione, ciascun assegnatario di carte di credito aziendali deve consegnarle all'Ufficio delle Risorse Umane, avvisando al contempo il Responsabile dell' Ufficio Payments & Cash, entro l'ultimo giorno di lavoro, unitamente a tutti i giustificativi delle spese sostenute per le quali non sono ancora state emesse fatture;
vi. l'Ufficio Payments & Cash provvede al blocco della carta di credito, comunicandolo all'emittente, il giorno stesso della consegna da parte dell'assegnatario per cessazione del rapporto di lavoro o collaborazione.

Con riferimento all'utilizzo di carte di credito aziendali, la Banca ha adottato i seguenti presidi e controlli:

i. ciascuna carta di credito viene emessa con limiti di utilizzo (CHF 30.000, Euro 25.000 e USD 25.000) ed eventuali maggiorazioni di tali limiti sono soggette ad una procedura specifica di approvazione da parte del responsabile diretto dell'assegnatario e del Capo Divisione di riferimento;
ii. ciascun assegnatario deve presentare mensilmente, per ciascuna spesa superiore a CHF 30, i giustificativi dei pagamenti effettuati, allegando la fattura di utilizzo della carta emessa dall'istituto emittente, i motivi dei pagamenti e il luogo di utilizzo;
iii. i pagamenti effettuati tramite carte di credito aziendali sono sottoposti ad una procedura di controllo, approvazione e pagamento delle fatture emesse da parte dell'istituto emittente;
iv. in caso di utilizzo di carte di credito aziendali oltre i limiti di importo o per motivi diversi da quelli consentiti, l'assegnatario è tenuto al rimborso delle spese sostenute entro 30 gg dalla data di emissione della fattura da parte dell'istituto emittente;
v. in caso di ripetuti abusi nell'utilizzo della carta di credito la Banca provvede al ritiro della stessa.

b. *Emissione e rilascio di carte di pagamento a favore dei clienti*

La Banca, non emettendo direttamente carte di pagamento, ha stipulato con istituti autorizzati accordi quadro per l'emissione delle stesse, da offrire alla propria clientela.

La Banca si è dotata di procedure interne per il rilascio di carte di pagamento a favore della clientela - che pur differenziandosi in alcuni processi a seconda della tipologia di carta rilasciata - prevedono in generale i seguenti presidi:

i. il rilascio di carte di pagamento è subordinato all'apertura di una relazione bancaria a nome del cliente e alla compilazione e sottoscrizione dell'apposito formulario, da consegnare, unitamente al documento identificativo, al funzionario clientela di riferimento;
ii. il funzionario della Banca, ricevuta la richiesta di rilascio della carta di pagamento, verifica che il formulario sia stato correttamente compilato dal cliente e lo trasmette all' Ufficio Payments & Cash;
iii. l' Ufficio Payments & Cash, previa verifica della completezza della documentazione ricevuta e dell'approvazione della linea di credito inerente alla carta di pagamento conformemente alle

competenze creditizie regolate all'interno del corpus normativo della Banca, provvede alla trasmissione della richiesta di rilascio di carta di pagamento e all'emittente della stessa;

iv. le carte di pagamento della clientela sono inviate in busta chiusa dall'emittente all'ufficio Payments & Cash;

v. i PIN delle carte di pagamento sono inviate tramite lettera coperti da sigillo dall'emittente direttamente all' ufficio Payments & Cash;

vi. le carte di pagamento sono registrate in apposito database, accessibile solo ai dipendenti dell'ufficio Payments & Cash e in cui sono riportati i dati dei titolari, delle carte di pagamento stesse e delle relative scadenze;

vii. l'ufficio Payments & Cash provvede alla consegna in buste chiuse, contenenti le carte di pagamento e i PIN, ai clienti secondo istruzioni dai medesimi ricevute:

   a. per posta raccomandata o corriere internazionale (se fuori dal territorio svizzero), all'indirizzo indicato dal cliente, provvedendo all'invio di due lettere, una contenente la carta di pagamento e l'altra contenente il PIN;

   b. presso la sede di Lugano, ove la carta di pagamento viene consegnata, dietro specifica richiesta scritta e previo rilascio di ricevuta di avvenuta consegna, da un incaricato dell' ufficio Payments & Cash al funzionario clientela. Quest'ultimo provvede alla consegna al cliente delle lettere contenenti la carta di pagamento e i PIN, raccogliendo la relativa ricevuta di consegna;

   c. presso le succursali, ove l'ufficio Payments & Cash, previa richiesta scritta da parte del funzionario clientela, provvede ad inviare, con due lettere separate, la carta di pagamento e il relativo PIN. Il funzionario clientela della succursale, ricevute le lettere, provvede al rilascio della relativa ricevuta di consegna. Al momento della consegna della carta di pagamento e del PIN al cliente il funzionario clientela richiede a quest'ultimo il rilascio della relativa ricevuta di consegna;

viii. l'ufficio Payments & Cash provvede alla conservazione in appositi dossier di tutta la documentazione relativa alla richiesta e alla consegna delle carte di pagamento di ciascun cliente;

ix. eventuali richieste di emissione di nuovi PIN sono trasmesse direttamente dal cliente all'emittente della carta di pagamento, senza intermediazione da parte della Banca.

c. *Gestione di sistemi di pagamento offerti alla clientela, diversi dalle carte di pagamento*

La Banca accetta disposizioni di pagamento da parte della propria clientela attraverso i seguenti strumenti:

- online, tramite accesso all'E-Banking da parte del cliente;
- e-mail e fax, trasmessi dal cliente al consulente;
- istruzioni in originale firmate dal cliente;
- ordini telefonici, comunicati dal cliente al consulente.

La Banca accetta istruzioni trasmesse tramite altri mezzi di comunicazione non menzionati sopra (quali per esempio: SMS, MMS, Whatsapp) solo se vi è una manleva telefonica in essere e una conseguente conversazione verbale registrata di conferma dell'istruzione da parte di una persona autorizzata.

Con specifico riferimento all'E-Banking, la Banca ha adottato i seguenti presidi:

- l'accesso all'E-Banking è consentito previa imputazione da parte del cliente delle credenziali di accesso (ID e password) ed inserimento di un codice OTP generato attraverso Token;
- le credenziali di accesso all'E-Banking vengono rilasciate dalla Banca al momento della richiesta di utenza e-banking; la password deve necessariamente essere modificata dal cliente al primo accesso;
- le disposizioni di pagamento possono essere effettuate esclusivamente attraverso l'imputazione di codici generati da *token* fisici o in forma di *mobile app* (c.d. "autenticazione forte"). I pagamenti devono essere autorizzati dagli utenti definiti del conto, secondo i poteri di disposizione dichiarati all'attivazione dell'e-banking;
- le disposizioni di pagamento tramite E-Banking sono eseguite automaticamente dal sistema informativo della Banca, senza alcun intervento manuale da parte della Banca stessa;
- su espressa richiesta del cliente, la Banca può resettare le credenziali di accesso all'E-Banking per crearne di provvisorie che devono essere necessariamente modificate dopo il primo accesso;
- le password ed i token dei clienti sono gestiti attraverso un sistema criptato, che garantisce la massima riservatezza degli stessi.

Con riferimento alle disposizioni di pagamento rilasciate dal cliente tramite e-mail e fax la Banca si è dotata dei seguenti presidi, meglio dettagliati nelle relative norme operative:

- il Cliente può trasmettere le disposizioni di pagamento al proprio consulente di riferimento o altro soggetto incaricato e previo rilascio di specifica informativa sui rischi connessi all'utilizzo di tale modalità di trasmissione e manleva a favore della Banca;
- tutte le istruzioni di pagamento sono soggette a verifica della conformità della firma dell'ordinante da parte dell'Ufficio Formalità prima della relativa esecuzione, in conformità con le relative norme operative interne;
- ricevuta l'email contenente una disposizione di pagamento, il consulente è obbligato necessariamente a procedere ad una verifica telefonica (*call back*) in base alle fattispecie indicate nella Norma Operativa 2.7;
- le disposizioni di pagamento via e-mail o fax sono stampate ed integrate con l'indicazione del giorno e dell'ora della chiamata di verifica; tale documentazione viene archiviata e conservata in appositi dossier;
- tutte le istruzioni non idonee ad essere accettate vengono comunque archiviate dall'Ufficio Formalità nel sistema informatico, con l'indicazione "da non eseguire" da parte del Consulente di riferimento
- accertata la correttezza e plausibilità della disposizione di pagamento, il consulente, a sua volta, provvede a trasmettere all'unità formalità clientela le informazioni ricevute, affinché la inserisca nel sistema per essere processata dall'unità Payments & Cash.

Con riferimento alle disposizioni di pagamento rilasciate dai clienti telefonicamente, la Banca ha adottato i seguenti presidi:

- le disposizioni di pagamento possono essere rilasciate via telefono esclusivamente ad alcuni soggetti autorizzati (con competenze diverse a seconda del valore dell'operazione) e previo rilascio di specifica informativa sui rischi connessi all'utilizzo di tale modalità di trasmissione e manleva a favore della Banca;

- gli ordini telefonici sono registrati e il consulente deve assicurarsi che nel corso della telefonata siano rilasciate informazioni idonee ad identificare l'ordinante. I mezzi di registrazione utilizzati assicurano la tracciabilità del giorno, l'ora e del recapito telefonico dal quale è arrivata la disposizione di pagamento;
- i soggetti autorizzati, che ricevono gli ordini di pagamento via telefono, li inseriscono nel sistema per essere successivamente processati dall'unità Payments & Cash;
- in caso di incertezza circa le istruzioni trasmesse telefonicamente, il consulente può successivamente richiedere (i) una conferma scritta e firmata o (ii) nel caso in cui ciò non sia possibile, una conferma tramite e-mail e fax.

Con riferimento alle istruzioni ricevute in originale (via posta o consegnate), la Banca ha adottato i seguenti presidi:

- tutte le istruzioni di pagamento pervenute in originale sono recapitate al Consulente di riferimento; in caso di mancata indicazione del Consulente di riferimento l'Ufficio Formalità Clientela provvede a recapitarle al Consulente competente o altro soggetto incaricato;
- tutte le istruzioni di pagamento sono soggette a verifica della conformità della firma dell'ordinante da parte dell'Ufficio Formalità prima della relativa esecuzione, in conformità con le relative norme operative interne;
- tutte le istruzioni di pagamento in originale, non idonee ad essere accettate vengono comunque archiviate dall'Ufficio Formalità nel sistema informatico, con l'indicazione "*da non eseguire*" da parte del Consulente di riferimento
- accertata la correttezza e plausibilità della disposizione di pagamento, il Consulente, a sua volta, provvede a trasmettere all'unità Formalità clientela le informazioni ricevute, affinché la inserisca nel sistema per essere processate dall'unità Payments & Cash.

d. *Installazione e gestione di hardware e software (in particolare quelli relativi a sistemi di pagamento)*

La Banca usufruisce per le proprie attività di Core Banking e E-Banking di software di terzi parti concessi in licenza d'uso, senza alcuna conoscenza da parte del personale della Banca dei relativi codici sorgente e con espresso divieto contrattuale di alterazione o modificazione degli stessi.

L'installazione e l'utilizzo dei software aziendali, così come le relative modifiche, sono preceduti dai seguenti processi:

- sono creati gruppi di lavoro per effettuare diverse fasi di test, qualitativi, di compatibilità e di sicurezza, ciascuna delle quali è soggetta ad autorizzazione;
- durante le fasi di test sono effettuati controlli da parte delle funzioni competenti;
- la messa in produzione del software è soggetta all'esito positivo dei test e dei controlli, nonché all'autorizzazione da parte delle funzioni competenti;
- qualsiasi modifica ai software aziendali è soggetta ai suddetti processi di test, controllo e autorizzazione.

Nell'ambito dell'installazione e dell'utilizzo dei software, sono posti in essere i seguenti presidi:

- qualsiasi utilizzo di software, concesso in licenza d'uso, è soggetta a preventiva autorizzazione e installazione da parte dell'ICT Information & Communication Technology per gli aspetti tecnici e dell'ufficio Sicurezza la definizione delle credenziali operative;

- è garantita la segregazione dei ruoli tra chi installa e chi gestisce / utilizza gli applicativi;
- tutti i software installati sui dispositivi aziendali sono mappati;
- tutte le attività di utilizzo dei software sono tracciate ai fini di controllo;
- sono previsti blocchi informatici all'installazione di software non autorizzati.

Al fine di prevenire manomissioni, gli accessi degli amministratori ai sistemi e/o gli accessi dei fornitori esterni, sono dotati di un sistema di screen recording. Gli accessi alle periferiche degli hardware non definiti nel perimetro dell'infrastruttura sono disabilitati. Ogni comportamento anomalo da parte degli utenti è monitorato ed eventualmente bloccato e segnalato.

e. *Gestione e controllo degli accessi ai sistemi informatici*

Con riferimento ai presidi e ai controlli adottati dalla Banca in relazione al processo di gestione e controllo degli accessi si rinvia a quanto presto dal Capitolo 2.3, paragrafo d) della Parte Speciale del presente Modello.

10. Delitti contro il patrimonio culturale (art. 25 septiesdecies)

10.1. Premessa

La presente Sezione della Parte Speciale si riferisce ai delitti contro il patrimonio culturale inclusi tra i reati presupposto del D.Lgs. 231/2001 dalla legge 22/2022.

Sebbene la Legge 22/2022 non fornisca una definizione di patrimonio culturale, è possibile ricavare tale definizione dal D.lgs. 42/2004 (Codice dei Beni Culturali e del paesaggio). Ai sensi del Codice dei beni culturali e del paesaggio, il patrimonio culturale è costituito dai beni culturali e dai beni paesaggistici; i quali sono rispettivamente definiti, dall'art. 2 del D.lgs. 42/2004, come "*le cose immobili o mobili che, ai sensi degli articoli 10 e 11, 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*" e "*gli 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*".

10.2. Fattispecie delittuose

Si riporta di seguito la descrizione delle fattispecie di reato per le quali la Banca è risultata esposta al rischio di responsabilità amministrativa.

10.2.1. Ricettazione di beni culturali (art. 518 quater c.p.)

L'articolo 518 quater c.p. punisce chi acquista, riceve, o occulta beni culturali provenienti da qualsiasi altro delitto, o comunque si intromette nel farli acquistare, ricevere od occultare. La condotta illecita è particolarmente ampia, potendo potenzialmente rientrare nell'ambito di applicazione del reato ogni negozio giuridico.

Per quanto concerne l'elemento soggettivo, assume rilevanza il dolo eventuale, in ragione della peculiarità del bene oggetto del negozio giuridico, il quale deve suscitare un sospetto sulla legittimità della provenienza in qualsiasi persona di media levatura intellettuale.

10.2.2. Falsificazione in scrittura privata relativa a beni culturali (art. 518 octies c.p.)

L'articolo 518 octies c.p. punisce la falsificazione di una scrittura privata avente ad oggetto beni culturali mobili. Oggetto materiale del reato è la scrittura privata relativa a beni culturali mobili. Il Codice dei beni culturali e del paesaggio, all'art. 64, obbliga alla consegna della documentazione che ne accerti l'autenticità o almeno la probabile attribuzione e la provenienza dell'opera o, in mancanza, al rilascio di una dichiarazione recante tutte le informazioni disponibili sull'autenticità o la probabile attribuzione e la provenienza.

La disposizione contiene due condotte tipiche:

- la prima consiste nel formare, in tutto o in parte, una scrittura privata falsa o nell'alterare, distruggere, sopprimere od occultare, in tutto o in parte, una scrittura privata vera. È richiesto il dolo specifico del far apparire lecita la provenienza del bene;
- la seconda punisce chi fa uso della scrittura privata falsa. In tal caso è richiesto il dolo generico.

10.2.3. Violazioni in materia di alienazione di beni culturali (art. 518 nonies c.p.)

L'articolo 518 nonies c.p. punisce le condotte di:

1) alienazione o immissione sul mercato non autorizzate di beni culturali;

2) omessa denuncia, nel termine di trenta giorni, degli atti di trasferimento della proprietà o della detenzione di beni culturali;

3) consegna di un bene culturale soggetto a prelazione da parte dell'alienante prima del decorso del termine di sessanta giorni.

Il reato è punito a titolo di dolo generico.

10.2.4. Importazione illecita di beni culturali (art. 518 decies c.p.)

L'articolo 518 decies c.p. punisce l'importazione di beni culturali provenienti da delitto, rinvenuti a seguito di ricerche svolte senza autorizzazione (se prevista dalla normativa del luogo del rinvenimento) o esportati da un altro Stato in violazione della legge in materia di protezione del patrimonio culturale di quello Stato.

Il reato è punito a titolo di dolo generico e si consuma al momento dell'introduzione del bene culturale nel territorio italiano.

10.2.5. Uscita o esportazione illecite di beni culturali (art. 518 undecies c.p.)

L'articolo 518 undecies c.p. punisce il trasferimento all'estero beni culturali, cose di interesse artistico, storico, archeologico, etnoantropologico, bibliografico, documentale o archivistico o altre cose oggetto di specifiche disposizioni di tutela ai sensi della normativa sui beni culturali, senza attestato di libera circolazione o licenza di esportazione e l'omesso rientro nel territorio italiano alla scadenza del termine, di beni culturali, cose di interesse artistico, storico, archeologico, etnoantropologico, bibliografico, documentale o archivistico o altre cose oggetto di specifiche disposizioni di tutela ai sensi della normativa sui beni culturali, per i quali siano state autorizzate l'uscita o l'esportazione temporanee, nonché nei confronti di chiunque rende dichiarazioni mendaci al fine di comprovare al competente ufficio di esportazione, ai sensi di legge, la non assoggettabilità di cose di interesse culturale ad autorizzazione all'uscita dal territorio nazionale.

Il reato è punito a titolo di dolo generico.

10.2.6. Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518 duodecies c.p.)

L'articolo 518 duodecies c.p. punisce il danneggiamento ed il deturpamento o imbrattamento del patrimonio culturale (quindi comprensivo sia di beni culturali sia dei beni paesaggistici) altrui o propri dell'autore del reato.

Il danneggiamento può consistere nel distruggere, disperdere, deteriorare, rendere in tutto o in parte inservibili o non fruibili i beni. La condotta è punita a titolo di dolo generico.

Il deturpamento o imbrattamento consiste nel rendere incompatibili i beni ad un uso coerente con il loro carattere storico o artistico ovvero pregiudizievole per la loro conservazione o integrità.

10.2.7. Contraffazione di opere d'arte (art. 518 quaterdecies c.p.)

L'articolo 518 quaterdecies c.p. punisce chi:

1) contraffà, altera o riproduce un'opera di pittura, scultura o grafica ovvero un oggetto di antichità o di interesse storico o archeologico;

2) altera o riproduce, pone in commercio, detiene per farne commercio, introduce a questo fine nel territorio dello Stato o comunque pone in circolazione, come autentici, esemplari contraffatti,

alterati o riprodotti di opere di pittura, scultura o grafica, di oggetti di antichità o di oggetti di interesse storico o archeologico;

3) conoscendone la falsità, autentica opere od oggetti contraffatti, alterati o riprodotti;
4) con un mezzo diverso dalla autenticazione (mediante altre dichiarazioni, perizie, pubblicazioni, apposizione di timbri od etichette o con qualsiasi altro mezzo), accredita o contribuisce ad accreditare, conoscendone la falsità, come autentiche opere od oggetti contraffatti, alterati o riprodotti.

10.2.8. Riciclaggio di beni culturali (art. 518 sexies c.p.)

L'articolo 518 sexies c.p. punisce la sostituzione o il trasferimento di beni culturali provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

È richiesto il dolo specifico, ossia la consapevolezza delle caratteristiche del bene.

10.3. Attività sensibili

La Banca risulta esposta al rischio di commissione dei reati contro i beni culturali nell'ambito delle seguenti attività di compravendita di opere d'arte e prestito di opere d'arte.

10.4. Principi comportamentali

È fatto divieto a tutti i destinatari, nell'ambito dello svolgimento delle attività della Banca, del presente Modello di:

- sottrarre e impossessarsi o appropriarsi di un bene culturale altrui o di proprietà della Stato italiano, senza autorizzazione;
- alienare o immettere sul mercato un bene culturale di proprietà della Banca senza richiedere le necessarie autorizzazioni e seguendo l'iter previsto dalla normativa;
- acquistare in nome e per conto della Banca beni culturali dalla provenienza incerta o che siano stati rinvenuti tramite ricerche non autorizzate;
- di modificare, alterare, distruggere, creare o riprodurre beni culturali o documenti attestanti l'autenticità di beni culturali della Banca o di terzi;
- ricevere a qualsiasi titolo beni culturali di comprovata provenienza illecita o di cui si sospetta della loro provenienza.

10.5. Principi procedurali

L'attività di prevenzione dei reati oggetto del presente Sezione di Parte Speciale si basa su un sistema di presidi previsti nella Norma operativa 5.52.4.1 "Opere d'arte" e dalla prassi interne

Di seguito si riportano i presidi che la Banca adotta in relazione alle diverse attività aziendali sensibili al fine di prevenire la commissione dei reati oggetto della presente Sezione di Parte Speciale.

Compravendita e prestito di opere d'arte.

La Banca, nell'ambito dell'acquisto di opere d'arte, per prassi interna adotta i seguenti presidi:

- l'acquisto e la vendita di beni culturali vengono comunicati all'ufficio Security & Logistics dal CEO della Banca;

- il processo di acquisto dell'opera è gestito da un addetto dell'ufficio Security & Logistics, al quale sono demandati i compiti di contattare il venditore, organizzare la spedizione dell'opera, attivare la copertura assicurativa e avviare le procedure interne di pagamento.
- tutta la documentazione relativa alle opere d'arte acquistate dalla Banca è custodita presso l'ufficio Security & Logistics;

Tutte le opere d'arte di proprietà della Banca, se non depositate nel locale Tesoro quadri della Banca, sono esposte presso gli uffici, nelle diverse sedi, della Banca o affidate in comodato d'uso a società del gruppo. Le opere d'arte sono annualmente controllate e censite all'interno di un apposito inventario da parte dell'ufficio Security & Logistics della Banca.

La Banca concede in prestito le proprie opere a musei e gallerie d'arte, per periodi di tempo limitati, previa specifica autorizzazione da parte dell'addetto dell'ufficio Security & Logistics, approvata dal CEO. In tali casi: (i) l'addetto dell'ufficio Security & Logistics cura l'organizzazione del prestito con l'espositore e del trasporto dell'opera stessa; (ii) tutti i prestiti sono contrattualizzati tra la Banca e le gallerie d'arte / musei; (iii) è prevista l'attivazione di una copertura assicurativa dell'Opera d'Arte.

La vendita di opere d'arte segue lo stesso iter autorizzativo indicato sopra in relazione all'acquisto.