Allianz Bank
Financial Advisors

Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001

Versione adottata con delibera del Consiglio di Amministrazione del 25 marzo 2021

Indice

Definizioni

ABI: Associazione Bancaria Italiana;

Allianz Bank o **Banca** o **Società**: Allianz Bank Financial Advisors S.p.A., con sede legale in Milano, Piazza Tre Torri, n. 3;

AGCM: Autorità Garante della Concorrenza e del Mercato;

Attività Sensibili: le attività di Allianz Bank nel cui ambito sussiste il potenziale rischio di commissione dei Reati;

AUI: Archivio Unico Informativo, formato e gestito a mezzo di sistemi informativi, nel quale gli intermediari conservano in modo accentrato tutte le informazioni acquisite nell'adempimento degli obblighi di identificazione e registrazione previsti dal Decreto Antiriciclaggio;

Capogruppo: Allianz S.p.A., con sede legale in Milano, Piazza Tre Torri, n. 3

CCNL: il Contratto Collettivo Nazionale di Lavoro delle Banche attualmente in vigore ed applicato da Allianz Bank;

Codice Etico e di Comportamento: codice comportamentale adottato dal Gruppo Allianz e pubblicato sul sito internet della Banca, contenente gli standard minimi che tutti i Destinatari sono tenuti a rispettare al fine di prevenire situazioni che potrebbero minare l'integrità del Gruppo;

Codice Anticorruzione: il codice anticorruzione adottato dal Gruppo Allianz;

Comitato Consultivo Controlli Interni e Rischi (già Comitato Audit): il Comitato Consultivo istituito da Allianz Bank con la delibera del Consiglio di Amministrazione del 27 Aprile 2004 e ss.mm.;

Consiglio di Amministrazione: il Consiglio di Amministrazione di Allianz Bank e i suoi membri;

CONSOB: Commissione Nazionale per le Società e la Borsa;

Consulenti: i soggetti che agiscono in nome e/o per conto di Allianz Bank in forza di un contratto di mandato o di altro rapporto contrattuale di collaborazione;

Consulente/i Finanziario/i o **Consulente/i Finanziario/i abilitato/i all'offerta fuori sede**: i soggetti (già noti come promotori finanziari) a cui Allianz Bank ha contrattualmente conferito l'incarico di consulente finanziario abilitato all'offerta fuori sede;

Datore di Lavoro: il soggetto titolare del rapporto di lavoro o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa in quanto titolare dei poteri decisionali e di spesa. In caso di affidamento di lavori a impresa appaltatrice o lavoratore autonomo all'interno della propria unità produttiva, assume il ruolo di Datore di Lavoro il committente con i conseguenti obblighi previsti dall'art. 26 del Decreto Sicurezza;

D.lgs. 231/2001 o Decreto: il decreto legislativo dell'8 giugno 2001, n. 231 e successive modificazioni e integrazioni;

D.lgs. 231/2007 o Decreto Antiriciclaggio: il decreto legislativo del 21 novembre 2007, n. 231, che ha recepito la direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca misure di esecuzione;

D.lgs. 81/2008 o Decreto Sicurezza: il decreto legislativo del 9 aprile 2008, n. 81 in materia di tutela della salute e della sicurezza nei luoghi di lavoro;

Destinatari: i Dipendenti e i membri degli Organi Sociali di Allianz Bank, nonché tutti i soggetti di volta in volta individuati dai singoli capitoli di Parte Speciale del Modello;

Dipendenti: i soggetti aventi un rapporto di lavoro subordinato con Allianz Bank, ivi compresi i Dirigenti;

Dirigenti: i soggetti che, in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attuano le direttive del Datore di Lavoro organizzando l'attività lavorativa e vigilando su di essa;

Documento di Valutazione dei Rischi o DVR: il documento redatto dal Datore di Lavoro contenente una relazione sulla valutazione dei rischi per la salute e la sicurezza durante il lavoro ed i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuale conseguente a tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, l'indicazione del nominativo RSPP, del RLS e del Medico Competente che ha partecipato alla valutazione del rischio, nonché l'individuazione delle mansioni che eventualmente espongono i Lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento;

Fornitori: tutti i soggetti, persone fisiche o giuridiche, che forniscono beni e/o servizi ad Allianz Bank;

Gruppo Allianz: il gruppo di cui Allianz Bank, quale società controllata al 100% da Allianz S.p.A. è parte, insieme alle società di diritto italiano controllate da Allianz S.p.A. ai sensi dell'articolo 2359, primo e secondo comma, del codice civile;

Gruppo Bancario: Allianz Bank e le società di diritto italiano controllate da Allianz Bank ai sensi dell'art. 2359, primo e secondo comma, del codice civile;

Lavoratori: i soggetti che, indipendentemente dalla tipologia contrattuale, svolgono un'attività lavorativa nell'ambito della Società;

Linee Guida: raccomandazioni delle associazioni di categoria sviluppate sistematicamente sulla base di conoscenze continuamente aggiornate e valide come, p.e., le Linee Guida dell'ABI per la costruzione dei modelli di organizzazione, gestione e controllo per il settore bancario *ex* articolo 6, co. 3, D.lgs. 231/2001;

Medico Competente: medico in possesso dei titoli e dei requisiti formativi e professionali di cui all'art. 38 del Decreto Sicurezza che collabora, secondo quanto previsto dall'art. 29 comma 1 del richiamato decreto, con il Datore di Lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la Sorveglianza Sanitaria;

Modello/i o **Modello/i 231**: il modello o i modelli di organizzazione, gestione e controllo previsti dal D.lgs. 231/2001;

Organi Sociali: il Consiglio di Amministrazione e il Collegio Sindacale di Allianz Bank e i loro singoli membri;

Organismo di Vigilanza o **Organismo**: l'organismo interno di controllo, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello nonché al relativo aggiornamento;

Pubblica Amministrazione o **PA**: la pubblica amministrazione e, con riferimento ai reati nei confronti della pubblica amministrazione, i pubblici ufficiali e gli incaricati di un pubblico servizio;

Partner: le controparti contrattuali di Allianz Bank, quali ad esempio fornitori (ivi inclusi gli *outsourcer* di servizi, esterni al Gruppo), distributori, sia persone fisiche sia persone giuridiche con cui la Banca addivenga a una qualunque forma di collaborazione contrattualmente regolata (p.e., associazione temporanea d'impresa, *joint venture*, consorzio, collaborazione in genere, fornitura, appalto, ecc.), ove destinati a cooperare con la Banca nell'ambito delle Attività Sensibili;

Processo Sensibile: i processi di Allianz Bank, che si estrinsecano in una o più Attività Sensibili, nel cui ambito sussiste il potenziale rischio di commissione dei Reati;

Rapporto Continuativo: rapporto di durata rientrante nell'esercizio dell'attività della Banca, che dia luogo a più operazioni di versamento, prelievo o trasferimento di mezzi di pagamento e che non si esaurisce in una sola operazione;

Reato/i o **Reato/i Presupposto**: le fattispecie di reato ai quali si applica la disciplina prevista dal D.lgs. 231/2001;

Responsabile Antiriciclaggio: funzione aziendale responsabile della gestione delle problematiche legate all'antiriciclaggio;

Rappresentante dei Lavoratori per la Sicurezza o **RLS**: il soggetto eletto o designato per rappresentare i Lavoratori in relazione agli aspetti della salute e sicurezza sul lavoro;

Responsabile del Servizio di Prevenzione e Protezione o **RSPP**: il soggetto in possesso delle capacità e dei requisiti professionali indicati nel Decreto Sicurezza, designato dal Datore di Lavoro, a cui risponde, per coordinare il Servizio di Prevenzione e Protezione;

Servizio di Prevenzione e Protezione o **SPP**: l'insieme delle persone, sistemi e mezzi esterni o interni alla Società finalizzati all'attività di prevenzione e protezione dei rischi professionali;

Sistema di Controllo Interno o **SCI**: il sistema di controllo interno esistente in Allianz Bank;

Società di Service: le società del Gruppo che svolgono attività di servizio in favore di Allianz Bank o di altre società del Gruppo;

Soggetti Apicali: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

Soggetti Subordinati: le persone sottoposte alla direzione o alla vigilanza di un Soggetto Apicale;

Soggetti Periferici: soggetti che vendono direttamente alla clientela i prodotti bancari per conto della Società, come, p.e., consulenti finanziari abilitati all'offerta fuori sede;

Stakeholder: tutti i soggetti portatori di interessi nei confronti della Banca, quali azionisti, propri clienti, dipendenti, Consulenti Finanziari abilitati all'offerta fuori sede, investitori, partner, fornitori, la Pubblica Amministrazione e le *Authority* che vigilano sul suo operato e la società civile in genere;

Testo Unico Bancario: il decreto legislativo 1 settembre 1993, n. 385 e le sue successive modifiche e integrazioni;

Unità di Informazione Finanziaria o **UIF**: la struttura nazionale, istituita presso la Banca d'Italia dal D.lgs. n. 231/2007, incaricata di ricevere dai soggetti obbligati, di richiedere ai medesimi, di analizzare e di comunicare alle autorità competenti le informazioni che riguardano ipotesi di riciclaggio o di finanziamento del terrorismo.

PARTE GENERALE

1. La normativa di riferimento

1.1. Il decreto legislativo 8 giugno 2001, n. 231

Il decreto legislativo 8 giugno 2001, n. 231, in attuazione della delega conferita al Governo con l'art. 11 della legge 29 settembre 2000, n. 300, disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica.

Il Decreto delinea i principi e i criteri di attribuzione della responsabilità a carico degli enti per una serie di Reati Presupposto, a condizione che siano commessi nell'interesse o a vantaggio degli enti da persone che agiscono per loro conto.

La responsabilità dell'ente, che si aggiunge – in via diretta e autonoma – a quella della persona fisica che ha commesso materialmente il Reato, sussiste se viene accertato un *deficit* nella sua organizzazione che ha reso possibile la commissione dell'illecito da parte della persona fisica (c.d. **colpa di organizzazione**), se, cioè, non ha implementato un apparato di regole, procedure e presidi precauzionali volti a minimizzare i rischi insiti nelle proprie Attività Sensibili.

In quest'ottica, il principale strumento a disposizione dell'ente per dimostrare l'assenza di profili di colpa di organizzazione – e non incorrere, quindi, nella responsabilità delineata dal D.lgs. 231/2001 – è costituito dall'adozione ed efficace attuazione, prima della commissione di un reato presupposto, di un modello di organizzazione, gestione e controllo idoneo a prevenirne la realizzazione.

1.2. I criteri di imputazione della responsabilità

Ai sensi dell'art. 5 del Decreto, può sorgere una responsabilità dell'ente per i Reati commessi nel suo interesse o vantaggio:

- da Soggetti Apicali, vale a dire il Presidente, gli Amministratori, i Direttori Generali, il Direttore di una filiale o di una divisione, nonché l'amministratore di fatto o il socio unico che si occupa della gestione;
- da Soggetti Subordinati, ossia i soggetti sottoposti alla direzione o alla vigilanza di un Soggetto Apicale, vale a dire tutti i soggetti aventi un rapporto funzionale con l'ente, ivi inclusi i Soggetti Periferici.

I concetti di interesse e vantaggio, contemplati nell'art. 5 del Decreto quali criteri - tra loro alternativi - di imputazione oggettiva dell'illecito all'ente, hanno significati diversi. L'**interesse** esprime la direzione finalistica della condotta della persona fisica ad arrecare un beneficio all'ente, da verificare secondo una prospettiva *ex ante* ("a monte" dell'evento). Tale direzione deve trovare riscontro nell'idoneità della condotta a produrre il beneficio per l'ente; non è, invece, richiesto che lo stesso venga effettivamente conseguito. Il **vantaggio** è il risultato materiale del reato, verificabile *ex post*: assume quindi connotati oggettivi e rileva anche se conseguito dall'ente nonostante la persona fisica non agisse nel suo interesse. I due requisiti dell'interesse e del vantaggio possono coesistere; è, tuttavia, sufficiente che ne ricorra solo uno per innescare la responsabilità dell'ente.

Gli articoli 6 e 7 del D.lgs. 231/2001 disciplinano invece i criteri di imputazione soggettiva dell'illecito all'ente. Tali criteri differiscono in base alla funzione svolta dall'autore del reato all'interno dell'organizzazione.

Se si tratta dei Soggetti Apicali, la responsabilità dell'ente è presunta, ma l'ente può andare esente da responsabilità se dimostra che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione di reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione, gestione e controllo;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo *sub* b);

Se, viceversa, il Reato è stato commesso da Soggetti Subordinati il meccanismo muta: la pubblica accusa deve provare la responsabilità dell'ente, dimostrando che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza che gravano sui Soggetti Apicali.

In sintesi: se autore del Reato è un Soggetto Apicale, grava sull'ente l'onere di dimostrare l'assenza di una propria colpa di organizzazione, secondo i criteri indicati dall'art. 6 del Decreto; di contro, se autore del Reato è un Soggetto Subordinato, grava sull'accusa l'onere di dimostrare una colpa di organizzazione dell'ente.

1.3. L'efficacia esimente del Modello

L'adozione e l'efficace attuazione del Modello 231, pur non costituendo un obbligo giuridico, costituiscono il principale strumento a disposizione dell'ente per rappresentare l'assenza di *deficit* organizzativi al proprio interno e, in definitiva, per andare esente dalla responsabilità stabilita dal Decreto.

Il Decreto non indica, tuttavia, analiticamente le caratteristiche e i contenuti del Modello: si limita a dettare alcuni principi di ordine generale e taluni vincoli essenziali di contenuto. In generale, 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, nonché a rilevare ed eliminare tempestivamente situazioni di rischio.

In particolare, deve: (**i**) individuare le Attività Sensibili nell'ambito delle quali possono essere commessi i Reati; (**ii**) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione alle Attività Sensibili; (**iii**) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei Reati Presupposto; (**iv**) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza delle prescrizioni del Modello; (**v**) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Con riferimento all'efficace attuazione del Modello, il Decreto prevede, inoltre, la necessità di una verifica periodica e di una modifica dello stesso in caso di mutamenti nell'organizzazione o nell'attività dell'ente o, ancora, qualora emergano lacune da correggere.

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

In particolare, ai sensi dell'art. 6, comma 2-*bis*, lett. a) del Decreto, il Modello deve prevedere uno o più canali che consentano tanto ai soggetti apicali, quanto ai soggetti subordinati, «*di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del […] decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte*». Taluni di questi canali di comunicazione devono anche garantire «*la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione*». Inoltre, il medesimo comma 2-*bis*, lett. b) del Decreto precisa che il Modello deve poi individuare almeno un canale alternativo di segnalazione «*idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante*». Ancora, sempre il nuovo comma

2-*bis* sancisce (alla lett. c) il divieto di atti di ritorsione o comunque discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

Si stabilisce poi (alla lett. d) che il Modello debba individuare, nell'ambito del sistema disciplinare adottato ai sensi del Decreto, sanzioni «*nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate*».

Lo stesso D.lgs. 231/2001, infine, nonché il relativo Regolamento di attuazione emanato con Decreto Ministeriale del 26 giugno 2003, n. 201, afferma che i Modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministri competenti, può formulare entro trenta giorni osservazione sulla idoneità dei Modelli a prevenire i Reati. Per tale ragione, nella predisposizione e nell'aggiornamento del presente Modello, la Banca si è ispirata anche alle Linee Guida pubblicate e aggiornate dall'ABI e, a titolo di completezza e confronto, da quelle pubblicate e aggiornate da Confindustria, salvo che per i necessari adattamenti dovuti alla particolare struttura organizzativa di Allianz Bank.

1.4. I reati presupposto

Ai sensi del D.lgs. 231/2001, la responsabilità amministrativa da reato degli enti può trarre origine esclusivamente dalla commissione di uno dei Reati Presupposto tassativamente indicati dalla legge.

In particolare, al momento dell'approvazione del presente Modello, i Reati Presupposto possono essere raggruppati nelle seguenti categorie: (**a**) reati contro la PA o che offendono interessi pubblici; (**b**) reati informatici e trattamento illecito di dati; (**c**) reati in materia di criminalità organizzata; (**d**) reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento; (**e**) reati contro l'industria e il commercio; (**f**) reati societari; (**g**) reati commessi con finalità di terrorismo e di eversione dell'ordine democratico; (**h**) reati di mutilazione genitale femminile; (**i**) reati contro la personalità individuale; (**j**) reati ed illeciti amministrativi di abuso di mercato; (**k**) reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; (**l**) reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio; (**m**) reati in materia di violazione del diritto di autore; (**n**) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria; (**o**) reati ambientali; (**p**) impiego di cittadini di paesi terzi il cui soggiorno è irregolare; (**q**) reati di razzismo e xenofobia; (**r**) frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati; (**r**) reati tributari; (**t**) reati di contrabbando; (**u**) reati transnazionali; (**v**) reati della filiera degli oli vergini di oliva.

Come si vedrà, a seguito del *risk assessment* condotto dalla Banca, non tutti i Reati sono stati considerati rilevanti e, per tale motivo, non sono inclusi tra quelli presi in considerazione nella Parte Speciale del Modello. Ad ogni modo, una precisa individuazione e descrizione di tutte le fattispecie criminose dalle quali potrebbe dipendere un addebito di responsabilità all'ente ai sensi del D.lgs. 231/2001 è contenuta nell'**Allegato I** del presente Modello intitolata «*Elenco dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. 231/2001*».

1.5. Le sanzioni

Il Decreto prevede le seguenti tipologie di sanzioni nei confronti dell'ente: (**i**) sanzioni pecuniarie; (**ii**) sanzioni interdittive; (**iii**) confisca; (**iv**) pubblicazione della sentenza.

i. **Le sanzioni pecuniarie**

Le sanzioni pecuniarie si applicano sempre, anche nel caso in cui la persona giuridica abbia riparato le conseguenze derivanti dal reato.

La commisurazione della sanzione segue un criterio bifasico: (a) determinazione del numero di quote nell'ambito della cornice edittale prevista per ciascun illecito. In generale, il numero di quote non può essere inferiore a 100 e

superiore a 1.000; nella determinazione del numero delle quote, in particolare, il giudice tiene conto della gravità del fatto, del grado della responsabilità dell'ente e dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti; e (b) attribuzione a ogni singola quota di un valore compreso tra un minimo di € 258,00 ed un massimo di € 1.549,00. Nel fissare l'importo della singola quota, il giudice valuta le condizioni economico-patrimoniali dell'ente.

In concreto, le sanzioni pecuniarie potranno, dunque, oscillare tra un minimo di € 25.822,84 (riducibili, ai sensi dell'art. 12 del Decreto, sino alla metà) ed un massimo di € 1.549.370,69.

ii. **Le sanzioni interdittive**

Le sanzioni interdittive si applicano ai soli illeciti che espressamente le contemplano purché (a) l'ente abbia tratto rilevante profitto dal reato; ovvero (b) vi sia stata reiterazione di illeciti. Tali sanzioni mirano a prevenire la reiterazione del reato e, quando applicate, si aggiungono alle sanzioni pecuniarie.

Tale categoria di sanzioni ricomprende le seguenti misure:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la Pubblica Amministrazione;
- l'esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o la revoca di quelli eventualmente già concessi;
- il divieto di pubblicizzare beni o servizi.

La durata delle misure interdittive è generalmente temporanea (da un minimo di 3 mesi ad un massimo di 2 anni), ad esclusione di alcuni casi tassativi nei quali le misure possono assumere carattere definitivo.

Inoltre, a seguito dell'entrata in vigore della legge 9 gennaio 2019, n. 3 (c.d. Legge "*Spazza-corrotti*"), fanno eccezione la concussione, la corruzione per un atto contrario ai doveri d'ufficio (anche nell'ipotesi aggravata ex art. 319-*bis* c.p.), la corruzione in atti giudiziari, l'induzione indebita a dare o promettere utilità e l'istigazione alla corruzione dal lato attivo, per le quali è prevista la durata delle sanzioni interdittive «*non inferiore a quattro anni e non superiore a sette*» e «*non inferiore a due anni e non superiore a quattro*», a seconda che il reato sia commesso da un Soggetto Apicale ovvero da un Soggetto Subordinato. Tuttavia, anche per queste fattispecie di reato, la durata delle sanzioni interdittive ritorna ad essere quella ordinaria sopra richiamata «*se prima della sentenza di primo grado l'ente si è efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi*».

Tuttavia, ai sensi del Decreto, l'ente non incorre in sanzioni interdittive, anche qualora siano astrattamente applicabili, se: (i) l'autore del reato ha agito nel prevalente interesse proprio e l'ente ha tratto un vantaggio minino dal reato; e (ii) il danno cagionato è di minima entità.

Inoltre, ferma l'applicazione delle sanzioni pecuniarie, le sanzioni interdittive non si applicano allorché, prima della dichiarazione di apertura del dibattimento di primo grado, concorrano le seguenti condizioni:

- l'ente abbia risarcito integralmente il danno ed abbia eliminato le conseguenze dannose o pericolose del reato, ovvero si sia comunque efficacemente adoperato in tal senso;
- l'ente abbia eliminato le carenze organizzative che hanno determinato il reato, mediante l'adozione di modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- l'ente abbia messo a disposizione il profitto conseguito ai fini della confisca.

Le sanzioni interdittive possono essere disposte anche in via cautelare.

iii. **La confisca**

Si tratta di una sanzione prevista come obbligatoria in caso di condanna dell'ente; consiste nell'ablazione del prezzo o del profitto del reato, ad esclusione della parte che può essere restituita al danneggiato. Qualora non sia possibile attingere direttamente il prezzo o il profitto del reato, la misura può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (c.d. confisca per equivalente o di valore).

Il Decreto prevede talune forme di confisca applicabili anche in assenza di sentenza di condanna:

- la prima ipotesi è contemplata dall'art. 6, comma 5: si prevede la confisca obbligatoria del profitto che l'ente ha tratto dal reato commesso da Soggetti Apicali, anche nel caso in cui l'ente non sia ritenuto responsabile dell'illecito. In tal caso, la confisca svolge una funzione di compensazione, necessaria per ristabilire l'equilibrio economico alterato dalla commissione del reato-presupposto;
- l'art. 15, comma 4, prevede altresì la confisca del profitto derivante dalla prosecuzione dell'attività dell'impresa nel caso questa sia affidata a un commissario giudiziale;
- infine, l'art. 23, comma 3, prevede la confisca del profitto derivato all'ente dalla prosecuzione dell'attività per l'ipotesi in cui l'ente, cui sia stata applicata una sanzione o una misura cautelare interdittiva, abbia violato gli obblighi o i divieti inerenti a tali sanzioni.

iv. La pubblicazione della sentenza

La pubblicazione della sentenza di condanna è disposta nel caso in cui nei confronti dell'ente venga disposta una sanzione interdittiva. La sentenza è pubblicata a spese della persona giuridica condannata, una sola volta, per estratto o per intero, in uno o più giornali indicati dal giudice nella sentenza di condanna, nonché mediante affissione nel Comune ove l'ente ha la sede principale.

1.6. I reati commessi all'estero

Secondo l'art. 4 del Decreto, l'ente può essere chiamato a rispondere in Italia in relazione ai Reati Presupposti commessi all'estero. La Relazione illustrativa al D.lgs. 231/2001 sottolinea – come *ratio* di tale opzione normativa – la necessità di non lasciare sfornita di sanzione una situazione di frequente verificazione, anche al fine di evitare facili elusioni dell'intero impianto normativo in esame.

Affinché possa sorgere una responsabilità dell'ente per reati commessi all'estero, è necessario che: (a) il reato sia commesso all'estero da un soggetto funzionalmente legato all'ente, ai sensi dell'art. 5, comma 1, del Decreto; (b) l'ente abbia la propria sede principale nel territorio dello Stato italiano; (c) ricorrano le condizioni previste dagli artt. 7, 8, 9 e 10 c.p.; (d) non stia già procedendo nei confronti dell'ente lo Stato nel quale è stato commesso il fatto; (e) se il reato presupposto è punibile a richiesta del Ministro della Giustizia, la richiesta sia formulata anche nei confronti dell'ente stesso.

1.7. Il procedimento di accertamento dell'illecito

La responsabilità per illecito amministrativo derivante da reato viene accertata nell'ambito di un procedimento penale.

A tale proposito, l'art. 36 D.lgs. 231/2001 prevede che «*la competenza a conoscere gli illeciti amministrativi dell'ente appartiene al giudice penale competente per i reati dai quali gli stessi dipendono. Per il procedimento di accertamento dell'illecito amministrativo dell'ente si osservano le disposizioni sulla composizione del tribunale e le disposizioni processuali collegate relative ai reati dai quali l'illecito amministrativo dipende*».

L'ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia imputato (o indagato, nella fase che precede l'esercizio dell'azione penale) del reato da cui dipende l'illecito amministrativo;

quando il legale rappresentante non compare, l'ente costituito è rappresentato dal difensore (art. 39, commi 1 e 4 D.lgs. 231/2001).

2. Il Modello di organizzazione, gestione e controllo di Allianz Bank

2.1. La struttura organizzativa di Allianz Bank

Allianz Bank Financial Advisors S.p.A. è la Banca del Gruppo Allianz che svolge attività bancaria e presta i servizi di investimento di cui all'articolo 1, commi 5 e 6, del D.lgs. n. 58/1998 e successive modifiche ed integrazioni.

La rete commerciale di Allianz Bank comprende alcune migliaia di Consulenti Finanziari. Gli sportelli operativi sul territorio nazionale e i diversi negozi completano la rete di distribuzione della Banca.

Quanto alla struttura aziendale di Allianz Bank, si rinvia all'organigramma aziendale, rinvenibile nell'**Allegato II** del presente Modello, e al «*Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma*» ove è descritta l'organizzazione della Banca nel suo complesso con la specificazione delle aree e delle relative funzioni.

La Banca detiene la partecipazione totalitaria nella società controllata RB Fiduciaria S.p.A. e una partecipazione nella società Investitori SGR S.p.A. ed è qualificata quale Capogruppo del gruppo bancario denominato "Gruppo Allianz Bank Financial Advisors", come tale iscritto all'albo previsto dall'art. 64 del D.lgs. 1 settembre 1993, n. 385.

2.2. Funzione e scopo del Modello

Il presente modello di organizzazione, gestione e controllo, adottato dal Consiglio di Amministrazione della Banca e periodicamente aggiornato, costituisce regolamento interno di Allianz Bank vincolante per la medesima: esso è inteso come l'insieme delle regole operative e delle norme deontologiche adottate dalla Banca al fine di prevenire la commissione dei Reati Presupposto ai sensi del Decreto.

Lo scopo del Modello è la costruzione di un sistema strutturato e organico di procedure e attività di controllo che abbia l'obiettivo di prevenire la commissione dei Reati, mediante l'individuazione delle Attività Sensibili maggiormente esposte a rischio di reato e la conseguente adozione degli opportuni presidi cautelari.

Attraverso l'adozione del Modello, quindi, la Banca si propone di perseguire le seguenti finalità:

- ribadire i valori di integrità e legalità che devono guidare l'attività di tutti i soggetti che operano per suo conto;
- ribadire che qualsiasi comportamento illecito è fortemente stigmatizzato dalla Banca, anche qualora possa arrecarle significativi benefici;
- chiarire ai Destinatari quali sono i comportamenti che potrebbero esporli a sanzioni penali e disciplinari e dai quali potrebbe sorgere anche una responsabilità amministrativa in capo alla Banca;
- fornire ai Destinatari un sistema di regole funzionali a minimizzare il rischio di incorrere in tali responsabilità;
- consentire alla Banca, grazie ad un'azione di monitoraggio sulle aree e i processi a rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei Reati presupposto.

L'adozione e l'efficace attuazione del Modello, non solo consentono a Allianz Bank di dimostrare l'assenza di una colpa d'organizzazione e non incorrere quindi in sanzioni ai sensi del D.lgs. 231/2001, ma migliorano anche la sua *corporate governance*.

L'efficacia del Modello è poi ulteriormente rafforzata dall'attività di vigilanza continua dell'Organismo di Vigilanza sul rispetto di tutte le direttive emanate direttamente dal Gruppo Allianz SE, in materia di *corporate governance*, controllo interno, antifrode e anticorruzione.

2.3. La fasi di costruzione e di revisione del Modello

Successivamente all'emanazione del Decreto, la Banca ha avviato un progetto interno finalizzato alla predisposizione del Modello 231. A tale scopo Allianz Bank ha svolto una serie di attività propedeutiche, suddivise in differenti fasi, e dirette tutte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D.lgs. 231/2001 ed ispirate, oltre che alle norme in esso contenute ed al Modello della Capogruppo, anche alle Linee Guida ABI.

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

i. **Analisi del contesto aziendale e identificazione delle Attività Sensibili ("*as-is-analysis*")**

L'identificazione delle Attività Sensibili è stata svolta, con il supporto di Consulenti esterni, attraverso la collaborazione dei soggetti chiave nell'ambito della struttura aziendale, l'esame della documentazione aziendale disponibile (*i.e.*, organigrammi, attività svolte, processi principali, ecc.) ed una serie di interviste.

Dallo svolgimento di tale processo di analisi è stato possibile individuare, all'interno della struttura aziendale, una serie di Attività Sensibili nel compimento delle quali si potrebbe eventualmente ipotizzare, quantomeno in astratto, la potenziale commissione di Reati Presupposto. Successivamente, con il supporti dei citati soggetti chiave, si è proceduto a valutare le modalità di gestione delle Attività Sensibili, il sistema di controllo sulle stesse (*e.g.*, procedure esistenti, separazione delle funzioni, tracciabilità documentale dei controlli, ecc.), nonché la conformità di quest'ultimo ai principi di controllo interno comunemente accolti (*e.g.*, verificabilità, tracciabilità, documentabilità, ecc.).

Obiettivo di questa fase è stata l'analisi del contesto aziendale al fine di identificare in quali aree e/o settori di attività e secondo quali modalità si potessero realizzare Reati Presupposto.

ii. **Effettuazione della c.d. *gap analysis***

Sulla base dei sistemi di controlli e delle procedure esistenti in relazione alle Attività Sensibili e delle previsioni e finalità del Decreto, si sono individuate le azioni di miglioramento dell'attuale sistema di controllo interno e dei requisiti organizzativi per la definizione di un Modello ai sensi del D.lgs. 231/2001; i risultati di tale attività sono stati esposti in un documento di *Executive Summary*.

Le fasi di identificazione delle Attività Sensibili e di effettuazione della *Gap Analysis* sono state svolte su base annua e ogniqualvolta si è reso necessario aggiornare e integrare il Modello attraverso l'emanazione di successivi capitoli di Parte Speciale in relazione alle diverse tipologie di reato di volta in volta introdotte dal legislatore.

iii. **Attività di *risk assessment* e aggiornamento periodico**

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

A tale scopo, la Banca svolge una serie di attività dirette sia all'aggiornamento del Modello – nella sua Parte Generale e Speciale – sia alla valutazione dei rischi di commissione dei Reati, al fine di identificare eventuali punti di miglioramento nell'ambito dei presidi di controllo definiti dalla Banca.

In breve, l'attività di aggiornamento e *Risk Assessment* di delinea nelle seguenti fasi:

a) mappatura, per ogni famiglia di illecito, all'interno di apposite matrici, delle Attività Sensibili, dei principi e delle procedure adottate dalla Banca e poste a mitigazione del rischio di commissione dei Reati Presupposto;

b) condivisione delle schede e conduzione di apposite interviste con le funzioni aziendali coinvolte nelle Attività Sensibili mappate al fine di raccogliere (b.1) riscontri circa la correttezza e la completezza, in base alla propria conoscenza ed esperienza, delle Attività Sensibili e dei presidi posti a mitigazione del rischio-

reato, così come riportati nel Modello; (b.2) indicazioni di modificazioni e/o integrazioni intervenute nell'ambito di presidi di controllo adottati dalla Banca a fronte di ciascuna Attività Sensibile; (b.3) valutazione degli elementi di rischio di commissione del Reato a cui è potenzialmente esposta ciascuna Attività Sensibile sulla base dell'esperienza e della conoscenza dei soggetti coinvolgi dalle attività di *business* svolte;

c) rielaborazione dei riscontri forniti al fine di (c.1) recepire all'interno del Modello eventuali modifiche o integrazioni indicate; (c.2) fornire una valutazione complessiva del rischio di commissione dei Reati e identificare eventuali punti di miglioramento nell'ambito dei presidi di controllo definiti dalla Banca.

2.4. La struttura del Modello

Il Modello 231 della Banca è costituito da:

i. una "**Parte Generale**", che descrive la normativa rilevante e le regole generali di funzionamento del Modello e dell'Organismo di Vigilanza;

ii. una "**Parte Speciale**", suddivisa per capitoli predisposti per ogni categoria di Reato contemplata nel D.lgs. 231/2001, focalizzata sulle aree di attività e sui processi ritenuti potenzialmente sensibili, con un'indicazione dei principi generali di comportamento da seguire per la prevenzione dei Reati Presupposto;

iii. l'**Allegato I** intitolato «*Elenco dei reati presupposto della responsabilità amministrativa degli enti ai sensi del D.lgs. 231/2001*»;

iv. l'**Allegato II** intitolato «*Organigramma di Allianz Bank Financial Advisors S.p.A.*»

Devono inoltre essere ritenuti parte integrante del Modello, anche per quanto si dirà *infra* §2.5, il **Codice Etico e di Comportamento** e il **Codice anticorruzione** adottati dal Gruppo Allianz e tutta la documentazione interna (p.e., funzionigrammi, processi, procedure, *template*, ecc.) della Banca richiamata nella Parta Speciale.

2.5. Natura, fonti e principi del Modello

Il presente Modello, come originariamente adottato dal Consiglio di Amministrazione della Banca e periodicamente aggiornato, costituisce un **regolamento interno** di Allianz Bank, vincolante per la medesima: esso è da intendersi come l'insieme delle regole operative e delle norme deontologiche adottate dalla Banca – in funzione delle specifiche attività svolte – al fine di prevenire la commissione dei Reati suscettibili di dare luogo a una responsabilità ai sensi del Decreto.

Il Modello è ispirato alle Linee Guida dell'ABI e fondato sulle risultanze della mappatura dei rischi sopra descritta.

Il **Codice Etico e di Comportamento** adottato dalla Banca costituisce fondamento essenziale del presente Modello: le disposizioni di quest'ultimo si integrano con quanto previsto nel Codice Etico e di Comportamento. In particolare, il Codice Etico e di Comportamento, i cui principi si intendono interamente richiamati nel presente Modello, contiene una serie di obblighi giuridici e doveri morali che definiscono l'ambito della responsabilità etica e sociale di ciascun partecipante all'organizzazione e che, nel loro complesso, costituiscono un efficace strumento volto a prevenire comportamenti illeciti o irresponsabili da parte dei soggetti che si trovano ad agire in nome e per conto della Banca.

Come osservato in precedenza, nella predisposizione del Modello si è tenuto conto delle procedure e dei sistemi di controllo esistenti e già ampiamente operativi nella Banca, in quanto idonei a valere anche come misure di prevenzione dei Reati Presupposto e di controllo sui processi coinvolti nelle Attività Sensibili.

Il presente Modello, quindi, ferma restando la sua peculiare funzione descritta *supra*, si inserisce nel più ampio sistema di controllo costituito principalmente dalle regole di *corporate governance* e dal Sistema di Controllo Interno esistente in Allianz Bank e delle relative procedure: tale sistema di controllo e le relative procedure, nella

versione di volta in volta esistente, è parte integrante del più ampio documento – il Modello 231, appunto – necessario ai fini del Decreto.

In particolare, sotto tale profilo, uno degli strumenti di carattere generale e avente rilievo nella Banca è il sistema di **deleghe aziendali**, sancito dall' art. 20 dello Statuto Sociale secondo il quale la rappresentanza legale della Banca, di fronte ai terzi ed in giudizio e la **firma sociale** spettano al Presidente e ai Vice Presidenti, se nominati, disgiuntamente fra loro e all'Amministratore Delegato nei limiti della delega conferita. L'amministratore Delegato potrà conferire, nell'ambito dei poteri a lui attribuiti, **deleghe** e **poteri di rappresentanza** della Banca, per singoli atti o categorie di atti, **procure** e **mandati speciali** a dipendenti della Banca e a terzi, anche con facoltà di subdelega.

Inoltre, quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali anche in relazione ai Reati Presupposto da prevenire, Allianz Bank, oltre al Codice Etico e di Comportamento, ha individuato:

- la circolare n. 285 emessa da Banca d'Italia il 17 dicembre 2013 e successive modificazioni e integrazioni, nonché in generale la normativa regolamentare vigente;
- il Sistema di Controllo Interno e, quindi, le **procedure aziendali** e di Gruppo, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale e organizzativa della Banca e del Gruppo e il sistema di controllo di gestione;
- le norme per l'erogazione del credito;
- le norme inerenti il sistema amministrativo, contabile, finanziario e di *reporting* del Gruppo;
- i principi contabili internazionali – *i.e.*, gli *International Accounting Standards* (IAS) e gli *International Financial Reporting Standards* (IFRS) – nonché le loro successive modifiche e relative interpretazioni;
- le comunicazioni e circolari aziendali ai Dipendenti e ai Consulenti Finanziari;
- la formazione dei Dipendenti e dei Consulenti Finanziari;
- il sistema sanzionatorio di cui al CCNL;
- il sistema di deleghe, disposizioni e procedure aziendali poste a presidio delle Attività Sensibili richiamate nella Parte Speciale del presente Modello;
- in generale, la normativa italiana e straniera applicabile.

Le regole, procedure e principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello, ma fanno parte del più ampio sistema di organizzazione e controllo della Banca che lo stesso intende integrare e sono costantemente aggiornati dalle funzioni aziendali a ciò preposte.

Tutto ciò premesso, e fermo quanto previsto *supra* §2.2, i **principi cardine** del presente Modello, quindi, sono:

i. le Linee Guida, in base alle quali è stata predisposta la mappatura delle Attività Sensibili della Banca e i Reati Presupposto astrattamente rilevanti;

ii. i requisiti indicati dal D.lgs. 231/2001 e, in particolare (a) l'attribuzione a un Organismo di Vigilanza, interno alla struttura aziendale di Allianz Bank, del compito di attuare in modo efficace e corretto il Modello, anche attraverso il monitoraggio dei comportamenti aziendali e il diritto ad avere una informazione costante sulle attività rilevanti ai fini del Decreto; (b) la messa a disposizione dell'Organismo di Vigilanza di risorse aziendali di numero e valore ragionevole e proporzionato ai compiti affidatigli e ai risultati attesi e ragionevolmente ottenibili; (c) l'attività di verifica del funzionamento del Modello con conseguente aggiornamento periodico; (d) l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;

iii. i principi generali su cui si fonda un adeguato sistema di organizzazione aziendale, ossia il rispetto dei requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, in particolare per quanto

attiene all'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative;

iv. i principi generali di un adeguato sistema di controllo interno e, in particolare, la verificabilità e documentabilità di ogni operazione rilevante ai sensi del Decreto, il rispetto del principio di separazione delle funzioni, la definizione di poteri autorizzativi coerenti con le responsabilità assegnate, la comunicazione all'Organismo di Vigilanza delle informazioni rilevanti;

v. inoltre, con particolare riferimento alle attività esternalizzate, il sistema di organizzazione e controllo aziendale, in considerazione delle responsabilità che ne possono derivare, si ispira ai seguenti principi: (a) individuazione specifica dei ruoli e delle responsabilità dei soggetti coinvolti nello svolgimento delle attività; (b) tracciabilità dei processi aziendali affidati in *outsourcing*; (c) definizione delle modalità e dei livelli di qualità del servizio; (d) istituzione di flussi informativi tra l'*outsourcer* di servizi e il soggetto o la funzione aziendale esternalizzante;

vi. infine, il Sistema di Controllo Interno, pur nella doverosa opera di verifica generale dell'attività sociale, deve dare priorità nella sua attuazione alle aree in cui vi è probabilità più alta di commissione dei Reati Presupposto e una rilevanza più alta delle Attività Sensibili.

2.6. Adozione e aggiornamento del Modello

Allianz Bank è sensibile all'esigenza di assicurare il massimo grado di correttezza e trasparenza nello svolgimento delle attività aziendali, a tutela della propria immagine, delle aspettative dei propri azionisti e degli *stakeholders* ed è consapevole dell'importanza di dotarsi di un sistema di controllo interno idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri Dipendenti.

Per tale ragione, sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e Allianz Bank, come evidenziato in precedenza, possegga già un apparato di autoregolamentazione funzionale a garantire l'integrità e il rispetto della legge nel contesto aziendale, la Banca - proprio nella prospettiva di effettuare ogni sforzo teso al perseguimento dei valori nei quali crede - ha ritenuto opportuno dotarsi di un proprio Modello già con la delibera del Consiglio di Amministrazione del 24 marzo 2005. Con la medesima delibera, la Banca ha altresì istituito il proprio Organismo di Vigilanza, con la determinazione dei relativi poteri.

Il Modello è, come anticipato, inoltre periodicamente aggiornato dal Consiglio di Amministrazione. In particolare, a seguito della sua originaria adozione, il Modello della Banca è stato successivamente modificato dalle delibere del Consiglio di Amministrazione del (**i**) 28 febbraio 2006; (**ii**) 31 marzo 2006; (**iii**) 29 febbraio 2008; (**iv**) 29 aprile 2010; (**v**) 26 febbraio 201; (**vi**) 28 maggio 2014; (**vii**) 25 maggio 2016; (**viii**) 29 maggio 2017; (**ix**) 30 gennaio 2018 e, da ultimo, (**x**) 25 marzo 2021.

In particolare, in conformità alle prescrizioni dell'art. 6, co. 1, lett. a), del Decreto, essendo il Modello un atto di emanazione dell'organo dirigente, sono rimesse alla competenza esclusiva del Consiglio di Amministrazione tutte le modifiche e le integrazioni di carattere *sostanziale* dello stesso.

Nello specifico, il Consiglio di Amministrazione modifica tempestivamente il Modello qualora siano state individuate, dall'Organismo di Vigilanza o da altra funzione competente della Banca o da qualsiasi altro soggetto della stessa, significative violazioni o elusioni delle prescrizioni in esso contenute, che ne evidenziano l'inadeguatezza, anche solo parziale, a garantire l'efficace prevenzione dei Reati Presupposto. Inoltre, il Consiglio di Amministrazione aggiorna tempestivamente, in tutto o in parte, il Modello, anche su proposta dell'Organismo di Vigilanza, qualora intervengano mutazioni o modifiche: (**i**) nel sistema normativo e regolamentare che disciplina l'attività della Banca; (**ii**) nella struttura societaria e nell'organizzazione o articolazione della Banca; (**iii**) nell'attività della Banca o dei suoi beni e/o servizi offerti alla clientela; (**iv**) in riferimento ad altri e diversi elementi e circostanze che si dovessero ritenere essenziali per l'esito della mappatura dei rischi periodica.

Le proposte di modifica del Modello, anche quando non attivate dall'Organismo di Vigilanza, sono sempre preventivamente comunicate all'Organismo il quale deve tempestivamente esprimere un parere in merito.

Viceversa, l'Amministratore Delegato della Banca può apportare al Modello modifiche di natura puramente *formale*, qualora esse risultino necessarie per una migliore chiarezza ed efficienza. Le modifiche sono comunque immediatamente comunicate all'Organismo di Vigilanza e, per la sua ratifica, al Consiglio di Amministrazione.

Nello svolgimento del proprio incarico, l'Organismo di Vigilanza deve prontamente segnalare, in forma scritta, al Presidente del Consiglio di Amministrazione e all'Amministratore Delegato, i fatti che suggeriscono l'opportunità o la necessità di modifica o revisione del Modello. Il Presidente del Consiglio di Amministrazione, in tal caso, deve convocare la riunione del Consiglio di Amministrazione, affinché lo stesso adotti le deliberazioni di sua competenza.

Quanto sopra previsto si applica, in quanto compatibile, per l'adozione, ad opera delle articolazioni funzionali interessate, di nuove procedure o per le modifiche di procedure esistenti, necessarie per l'attuazione del Modello. In particolare, ancor prima dell'eventuale passaggio consiliare per la loro approvazione, le procedure di attuazione del Modello sono predisposte o aggiornate dalle competenti funzioni aziendali e prontamente trasmesse all'Organismo di Vigilanza.

2.7. Destinatari del Modello

Le regole contenute nel Modello si applicano in via diretta:

- **i.** a coloro che svolgono, anche di fatto, funzioni di rappresentanza, gestione, amministrazione, direzione e controllo della Banca o di una unità funzionale o di una divisione di questa, dotata di autonomia finanziaria;
- **ii.** ai Dipendenti della Banca, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale, ancorché distaccati all'estero per lo svolgimento delle loro attività;
- **iii.** ai Consulenti Finanziari della Banca.

La Banca riprova e sanziona qualsiasi comportamento contrario, oltre che alla legge, alle previsioni del Modello e del Codice Etico e di Comportamento, e così pure i comportamenti posti in essere al fine di eludere la legge, il Modello o il Codice Etico e di Comportamento, anche qualora la condotta sia realizzata nella convinzione che essa, anche in parte, persegue l'interesse della Banca ovvero con l'intenzione di arrecarle un vantaggio.

Il Modello della Banca è pubblicato sul sito *internet* aziendale www.allianzbank.it.

2.7.1. Rapporti con le Società di Service

Le Società di Service devono essere informate dell'avvenuta adozione del Modello e dell'esigenza per Allianz Bank che il loro comportamento sia conforme ai disposti del D.lgs. 231/2001, nonché a quelli del Codice Etico e di Comportamento.

2.7.2. Rapporti con Consulenti, *Partner* e Fornitori

In relazione ai rapporti instaurati con i Consulenti, i *Partner* e i Fornitori, a cura delle competenti direzioni o unità organizzative, sono istituiti appositi sistemi di valutazione per la selezione dei medesimi e per l'informativa nei loro confronti.

In ogni caso nei contratti con Consulenti, *Partner* e Fornitori dovranno essere inserite specifiche clausole con cui gli stessi si obbligano al rispetto dei principi dettati dal D.lgs. 231/2001 e dal Modello.

3. I processi sensibili e i reati presupposto rilevanti di Allianz Bank

3.1. I processi sensibili di Allianz Bank

A seguito delle analisi condotte da Allianz Bank e descritte nel precedente capitolo, ai fini della individuazione delle aree di rischio potenzialmente rilevanti ai sensi del Decreto, è emerso che i Processi Sensibili della Banca sono, alla data del presente Modello, i seguenti:

I. Gestione degli adempimenti e dei rapporti con gli enti pubblici e le autorità amministrative indipendenti, anche in occasione di verifiche ispettive;

II. Gestione dei flussi monetari e finanziari;

III. Selezione e gestione dei Consulenti Finanziari;

IV. Formazione del bilancio e gestione degli adempimenti societari e dei rapporti con gli organi di controllo;

V. Commercializzazione dei prodotti bancari, finanziari e assicurativi;

VI. Gestione dell'erogazione del credito;

VII. Acquisto di beni, servizi e consulenze;

VIII. Selezione, assunzione e gestione del personale;

IX. Gestione di omaggi, delle sponsorizzazioni e altre liberalità;

X. Gestione del contenzioso;

XI. Utilizzo dei sistemi informativi aziendali;

XII. Gestione dei rapporti con i *media* e delle informazioni privilegiate;

XIII. Adempimenti in materia di salute e sicurezza sui luoghi di lavoro *ex* D.lgs. 81/2008;

XIV. Gestione degli impatti ambientali generati dalle attività e dai processi;

XV. Gestione degli investimenti;

XVI. Gestione e rispetto della proprietà industriale e intellettuale;

XVII. Gestione della fiscalità aziendale.

Qualora uno o più dei Processi Sensibili si inserisca nel più ampio ambito delle **prestazioni infragruppo** tra la Compagnia e le sue controllate ovvero tra la Banca e le sue partecipate, insieme alle prescrizioni che verranno dettagliate nella Parte Speciale in relazione a ogni categoria di Reati Presupposto ritenuta rilevante, resta fermo l'obbligo di rispettare i seguenti principi generali:

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

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

3.2. I reati presupposto considerati rilevanti per Allianz Bank

Nondimeno, sempre a seguito delle analisi condotte dalla Banca e descritte nel capitolo precedente, è emerso che i Processi Sensibili sopra individuati possono astrattamente riguardare le seguenti categorie di Reati Presupposto:

1. Reati contro la Pubblica Amministrazione e quelli contro il patrimonio commessi a danno dello Stato o di altro ente pubblico *ex* artt. **24** e **25**, D.lgs. 231/2001, ad esclusione dei reati di «*Frode nelle pubbliche forniture*» (art. 356 c.p.), di quello di frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (art. 2, L. 898/1996), di «*Peculato*» (art. 314 c.p.), di «*Peculato mediante profitto dell'errore altrui*» (art. 316 c.p.), di «*Concussione*» (art. 317 c.p.) e di «*Abuso d'ufficio*» (art. 323 c.p.);
2. Reati informatici e di trattamento illecito dei dati *ex* art. **24-*bis***, D.lgs. 231/2001, ad esclusione dei reati di «*Frode informatica del certificatore di firma elettronica*» (art. 640-*quinquies* c.p.) e di quello in materia di «*Perimetro di sicurezza nazionale cibernetica*» (art. 1, co. 11, D.L. 105/2009 conv. dalla L. 133/2019);
3. Delitti di criminalità organizzata *ex* art. **24-*ter***, D.lgs. 231/2001, limitatamente all'ipotesi di «*Associazione per delinquere*» (art. 416 c.p.);
4. Reati di contraffazione *ex* **art. 25-*bis*.**, D.lgs. 231/2001, limitatamente alle ipotesi di «*Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate*» (art. 453 c.p.), «*Spendita e introduzione nello Stato, senza concerto, di monete falsificate*» (art. 455 c.p.), «*Spendita di monete falsificate ricevute in buona fede*» (art. 457 c.p.) e «*Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni*» (art. 473 c.p.)
5. Reati societari *ex* **art. 25-*ter***, D.lgs. 231/2001, ad esclusione del reato di «*Indebita ripartizione dei beni sociali da parte dei liquidatori*» (art. 2633 c.c.);
6. Delitti con finalità di terrorismo o di eversione dell'ordine democratico *ex* **art. 25-*quater***, D.lgs. 231/2001, limitatamente alle ipotesi di «*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*» (art. 270-*bis* c.p.) e di «*Finanziamento di condotte con finalità di terrorismo*» (art. 270-*quinquies*.1 c.p.);
7. Delitti contro la personalità individuale *ex* **art. 25-*quinquies***, D.lgs. 231/2001, limitatamente all'ipotesi di «*Intermediazione illecita e sfruttamento del lavoro*» (art. 603-*bis* c.p.);
8. Abusi di mercato *ex* **art. 25-*sexies***, D.lgs. 231/2001;
9. Reati di omicidio colposo e di lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro *ex* **art. 25-*septies***, D.lgs. 231/2001;
10. Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio *ex* **art. 25-*octies***, D.lgs. 231/2001;
11. Delitti in materia di violazione del diritto d'autore *ex* **art. 25-*novies***, D.lgs. 231/2001, ad esclusione delle violazioni nei confronti della Società Italiana degli Autori ed Editori di cui all'art. 171-*septies*, L. 633/1941 e del reato di manomissione di apparati per la decodificazione di segnali audiovisivi ad accesso condizionato (art. 171-*octies*, L. 633/1941);
12. Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria *ex* **art. 25-*decies***, D.lgs. 231/2001;
13. Reati ambientali *ex* **art. 25-*undecies***, D.lgs. 231/2001, limitatamente alle ipotesi di «*Inquinamento ambientale*» (art. 452-*bis* c.p.), di «*Delitti colposi contro l'ambiente*» (art. 452-*quinquies*, c.p.), di «*Attività organizzate per il traffico illecito di rifiuti*» (art. 452-*quaterdecies*, c.p.), degli illeciti in materia di gestione non autorizzata di rifiuti (art. 256, D.lgs. 152/2006), delle violazioni degli obblighi di comunicazione, di tenuta dei registri e dei formulari (art. 258, D.lgs. 152/2006), del reato di «*Traffico illecito di rifiuti*» (art.

259, D.lgs. 152/2006) e delle violazioni relative al sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-*bis*, D.lgs. 152/2006);

14. Dei reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare *ex* **art. 25-*duodecies***, D.lgs. 231/2001, limitatamente alla ipotesi di cui all'art. 22, co. 12-*bis*, D.lgs. 286/1998;

15. Reati tributari *ex* **art. 25-*quinquiesdecies***, D.lgs. 231/2001, ad esclusione del delitto di «*Dichiarazione infedele*» (art. 4 D. Lgs. 74/2000), «*Omessa dichiarazione*» (art. 5 D. Lgs. 74/2000) e «*Indebita compensazione*» (art. 10-*quater* D. Lgs. 74/2000).

Ogni categoria di Reato Presupposto considerato astrattamente rilevante per la Banca, sarà, di riflesso, oggetto di specifico approfondimento nella Parte Speciale.

Viceversa, non sono state individuate aree di attività della Società potenzialmente legate alle categorie di reati contro l'industria e il commercio *ex* art. 25-*bis.*1, D.lgs. 231/2001, alle pratiche di cui all'art. 25-*quater.*1, D.lgs. 231/2001, a quella relativa ai reati di razzismo e xenofobia di cui all'art. 25-*terdecies*, D.lgs. 231/2001, alle frodi sportive previste dall'art. 25-*quaterdecies*, D.lgs. 231/2001, nonché ai reati in materia di contrabbando di cui all'art. 25-*sexiesdecies* del Decreto.

4. L'Organismo di Vigilanza di Allianz Bank

4.1. Requisiti e composizione

In base all'art. 6, co. 1, lett. b), D.lgs. 231/2001, l'organo cui affidare il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento, deve essere un organismo dell'ente, dotato di autonomi poteri di iniziativa e di controllo. A tal riguardo si richiamano anche le disposizioni della Circolare n. 285 del 17 dicembre 2013 di Banca D'Italia recante «*Disposizioni di vigilanza per le banche*», secondo cui «*l'organo con funzione di controllo svolge, di norma, le funzioni dell'organismo di vigilanza – eventualmente istituito ai sensi del d.lgs. n. 231/2001, in materia di responsabilità amministrativa degli enti - che vigila sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione di cui si dota la banca per prevenire i reati rilevanti ai fini del medesimo decreto legislativo. Le banche possono affidare tali funzioni a un organo appositamente istituito dandone motivazione*» (Titolo IV, Capitolo 3, Sezione II, Paragrafo 4).

Pertanto Banca d'Italia, pur rispettando l'autonomia delle banche nella scelta di nominare organismi di vigilanza composti da soggetti diversi dai sindaci (facoltà esercitabile dandone adeguata motivazione), ha esplicitamente espresso il proprio favore per la coincidenza dell'Organismo di Vigilanza con l'organo di controllo, ossia il Collegio Sindacale (nei sistemi di governance tradizionale), al Consiglio di Sorveglianza (nei sistemi di governance dualistici) o al Comitato per il Controllo sulla Gestione (nei sistemi di governance monistici).

In tale ambito, Allianz Bank, con delibera dell'Assemblea degli azionisti, in data 28 aprile 2014 ha affidato le funzioni di vigilanza e controllo del Modello al **Collegio Sindacale della Banca**. Tale affidamento risulta essere in linea con le considerazioni espresse nell'ambito dalle Linee Guida ABI nelle quali, sulla base del testo formale del Decreto, unitamente alle considerazioni espresse sul punto dalla Relazione illustrativa al Decreto medesimo, si suggeriscono i requisiti di autonomia, indipendenza, onorabilità, professionalità e continuità di azione che devono caratterizzare l'Organismo.

i. Autonomia

Il requisito di autonomia presuppone che l'Organismo riferisca, per l'effettivo svolgimento delle sue funzioni, solo al massimo vertice gerarchico (ad esempio, Amministratore Delegato, Consiglio di Amministrazione e Comitato Consultivo Controlli Interni e Rischi); l'Organismo deve, inoltre, disporre di autonomi poteri di spesa ordinari e straordinari.

ii. Indipendenza

L'indipendenza, invece, presuppone che i componenti dell'Organismo non si trovino in una posizione, neppure potenziale, di conflitto di interessi con la Banca, né siano titolati all'interno della stessa di funzioni di tipo operativo.

iii. Onorabilità e cause di ineleggibilità

Il requisito dell'onorabilità presuppone l'assenza di cause di ineleggibilità o di decadenza, elencate nel prosieguo.

i. Professionalità

L'Organismo di Vigilanza deve possedere, al suo interno, competenze tecnico-professionali adeguate alla funzione che è chiamato a svolgere. Tali caratteristiche, unite alla indipendenza, garantiscono l'obiettività di giudizio; è necessario, pertanto, che all'interno dell'Organismo siano presenti soggetti con professionalità adeguate in materia giuridica, economica e di controllo e gestione dei rischi aziendali.

ii. Continuità d'azione

L'Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza sul Modello e la Banca gli garantisce i necessari poteri di indagine. È quindi una struttura riferibile alla Banca, in modo da garantire la dovuta continuità del suo lavoro, ma non svolge mansioni operative che possano condizionarne quella visione d'insieme sull'attività aziendale che si richiede all'Organismo.

Applicando tutti i citati requisiti alla realtà aziendale di Allianz Bank, i componenti dell'Organismo di Vigilanza sono nominati dall'Assemblea dei Soci in occasione della nomina del Collegio Sindacale, ai sensi della normativa *pro tempore* vigente, nonché in coerenza con le regole di *governance* illustrate nelle Linee Guida della Capogruppo. Nello specifico, alla data del presente Modello, l'Organismo di Vigilanza della Banca è composto da tre membri, coincidenti con i componenti del Collegio Sindacale. È Presidente dell'Organismo di Vigilanza il Presidente del Collegio Sindacale.

L'accettazione della (o cessazione dalla) carica di Sindaco comporta, pertanto, anche l'accettazione della (o cessazione dalla) carica di membro dell'Organismo di Vigilanza e delle relative responsabilità; il Collegio Sindacale svolge quindi le funzioni attribuite ai sensi del D.lgs. 231/2001 all'Organismo di Vigilanza per tutta la durata del proprio incarico.

Qualora nel corso dell'esercizio venissero a mancare uno o più Sindaci e nel Collegio Sindacale dovessero subentrare, ai sensi dell'art. 2401 c.c., i Sindaci supplenti, a questi ultimi si intenderanno estese automaticamente anche le funzioni di vigilanza e controllo proprie dell'Organismo di Vigilanza fino alla successiva nomina del Sindaco effettivo mancante.

Al fine di garantire i requisiti di **autonomia** e **indipendenza,** dal momento della nomina e per tutta la durata dell'incarico, i componenti dell'Organismo di Vigilanza:

- non devono rivestire incarichi esecutivi o delegati nel Consiglio di Amministrazione della Banca;
- non devono svolgere funzioni operative o di *business* all'interno della Banca;
- non devono intrattenere significativi rapporti d'affari con la Banca, con società da essa controllate o ad essa collegate o con Allianz S.p.A., salvo il rapporto di lavoro subordinato, né intrattenere significativi rapporti d'affari con gli amministratori muniti di deleghe (amministratori esecutivi);
- non devono avere rapporti con o far parte del nucleo familiare degli amministratori esecutivi, dovendosi intendere per nucleo familiare quello costituito dal coniuge non separato legalmente, dai partenti e affini entro il quarto grado;
- non devono risultare titolari, direttamente o indirettamente, di partecipazioni nel capitale della Banca;
- non devono essere stati condannati, con sentenza anche in primo grado, ovvero essere sottoposti a indagine, o aver ottenuto una sentenza di patteggiamento per la commissione di uno dei Reati, né tantomeno essere stati condannati a una pena che importi l'interdizione, anche temporanea, dai pubblici uffici.

Inoltre, non possono essere eletti membri dell'Organismo e, se lo sono, **decadono** automaticamente dalla carica:

- coloro che si trovano nelle condizioni previste dall'articolo 2382 c.c., ovverosia coloro che si trovano nella condizione di inabilitato, interdetto, fallito o condannato ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi;
- coloro che siano stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi del D.lgs. 6 settembre 2011, n. 159 «*Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia*»;
- coloro che 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:
    - per uno dei delitti previsti nel titolo XI del libro V del Codice Civile (Disposizioni penali in materia di società e consorzi) e nel regio decreto 16 marzo 1942 n. 267 (disciplina del fallimento, del concordato preventivo, dell'amministrazione controllata e della liquidazione coatta amministrativa);

- a pena detentiva, 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 di mercati e valori mobiliari, di strumenti di pagamento (tra questi si segnalano, a titolo esemplificativo e non esaustivo, i reati di abusivismo bancario e finanziario di cui agli artt. 130 e seguenti del Testo Unico Bancario, i reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate di cui all'art. 453 c.p., l'esercizio abusivo dell'attività assicurativa o riassicurativa ex art. 305 del Codice delle Assicurazioni Private - D.Lgs. 209/2005);
- per un delitto contro la pubblica amministrazione, o alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;
- alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;

- in ogni caso e a prescindere dall'entità della pena per uno o più illeciti tra quelli tassativamente previsti dal D. Lgs. n. 231/01;
- coloro che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto, salvo che siano trascorsi 5 anni dalla inflizione in via definitiva delle sanzioni ed il componente non sia incorso in condanna penale ancorché non definitiva;
- coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-*quater* TUF.

All'atto di nomina, i componenti dell'Organismo di Vigilanza sono tenuti a sottoscrivere una dichiarazione attestante l'esistenza dei requisiti sopra descritti e, comunque, a comunicare immediatamente al Consiglio di Amministrazione ed agli altri componenti dell'Organismo di Vigilanza l'insorgere di eventuali condizioni ostative.

L'Organismo di Vigilanza ha inoltre provveduto a darsi le proprie regole di funzionamento attraverso uno specifico regolamento denominato «*Regolamento interno per il funzionamento dell'Organismo di Vigilanza di Allianz Bank Financial Advisors* ex *D.lgs. 231/2001*», in linea con le regole di *corporate governance* di Allianz Bank.

Tenuto conto della peculiarità delle responsabilità attribuite all'Organismo di Vigilanza e dei contenuti professionali specifici da esse richiesti, nello svolgimento di compiti di vigilanza e controllo l'Organismo di Vigilanza di Allianz Bank è supportato, di norma, dalla funzione *Internal Auditing* – e, ove necessario, dalla funzione *Compliance* – e si può avvalere del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

L'Organismo potrà altresì coordinarsi con l'Organismo di Vigilanza della Capogruppo in un'ottica di omogeneità d'azione e di risultati.

L'Organismo può avvalersi inoltre del supporto di altre funzioni interne che, di volta in volta, si rendano necessarie allo svolgimento del suo incarico, ovvero ricorrere a Consulenti di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo.

All'Organismo di Vigilanza della Banca sono assegnate le risorse finanziarie necessarie per lo svolgimento delle attività e per l'efficiente ed effettivo assolvimento dei compiti cui esso è chiamato. L'entità della dotazione finanziaria ordinaria per ciascun esercizio viene proposta dall'Organismo al Consiglio di Amministrazione, in cui viene dato anche conto delle spese sostenute nell'esercizio precedente, e deve essere deliberata dal Consiglio di Amministrazione. Ove insorgano esigenze di spesa eccedenti l'entità delle risorse finanziarie assegnate all'Organismo, quest'ultimo potrà inoltrare una richiesta motivata al Consiglio di Amministrazione, per ottenere un'integrazione degli importi previsti a *budget*.

4.2. Funzioni e poteri

All'Organismo di Vigilanza della Banca è affidato il **compito** di vigilare: (**i**) sull'osservanza del Modello da parte dei Dipendenti, del Consiglio di Amministrazione e dei Consulenti Finanziari abilitati all'offerta fuori sede; (**ii**) sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale e alla effettiva capacità di prevenire la commissione dei reati; (**iii**) sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative, sollecitando a tal fine gli organi competenti.

Al fine di poter svolgere le proprie funzioni, all'Organismo sono affidati i seguenti **poteri**:

- **i.** in relazione alle *verifiche* e ai *controlli* funzionali all'efficace compimento del suo incarico, può: (**a**) valutare l'attuazione da parte della Banca delle procedure previste dalla Parte Speciale del Modello, anche tramite l'emanazione ovvero la proposizione di disposizioni interne volte al rispetto del Modello o delle procedure; (**b**) condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle Attività Sensibili; (**c**) effettuare periodicamente accertamenti mirati su determinate operazioni o su specifici atti posti in essere dalla Banca, soprattutto nell'ambito delle Attività Sensibili, i cui risultati devono essere riassunti in un'apposita relazione periodica da esporsi in sede di *reporting* agli organi societari deputati; (**d**) raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere messe a disposizione o trasmesse all'Organismo da parte degli altri organi e dalle funzioni sociali; (**e**) coordinarsi con le altre funzioni aziendali, anche attraverso apposite riunioni, per il miglior monitoraggio dell'operatività della Banca; (**f**) attivare e svolgere indagini interne raccordandosi di volta in volta con le funzioni aziendali interessare per acquisire ulteriori elementi di valutazione;
- **ii.** in relazione alla *formazione* in materia di responsabilità amministrativa da reato degli enti, può: (**a**) coordinarsi con la funzione Direzione Risorse per la definizione dei programmi di formazione e del contenuto delle comunicazioni periodiche per i Dipendenti e per gli Organi Societari, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base del Decreto; (**b**) coordinarsi con il Responsabile dell'Unità Organizzativa Sviluppo Professionale Risorse per la definizione dei programmi di formazione e del contenuto delle comunicazioni periodiche da inviare ai Consulenti Finanziari abilitati all'offerta fuori sede, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base del Decreto; (**c**) far predisporre e aggiornare lo spazio *intranet* della Banca contenente le informazioni relative al Decreto e al Modello; (**d**) monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;
- **iii.** in relazione a eventuali *mancato rispetto delle prescrizioni del Modello*, può coordinarsi con le funzioni aziendali competenti per valutare l'adozione di eventuali sanzioni o provvedimenti disciplinari, ferme restando le competenze delle stesse funzioni aziendali per l'irrogazione della misura adottabile e del relativo processo decisionale;
- **iv.** in relazione all'*aggiornamento del Modello*, può: (**a**) interpretare eventuali modifiche normative intervenute a seguito dell'approvazione del Modello, in coordinamento con l'Unità Organizzativa Legale, al fine di verificare l'adeguatezza dello stesso alle novità introdotte dal legislatore ovvero la necessità di modifiche; (**b**) valutare le eventuali ulteriori esigenze di aggiornamento e adeguamento del Modello, coordinandosi a tal fine anche con l'Organismo di Vigilanza della Capogruppo Allianz; (**c**) monitorare eventuali modifiche dell'organigramma aziendale e del Regolamento Interno per l'ordinamento ed il funzionamento della Struttura Organizzativa e del Progetto di Governo Societario, ove è descritta l'organizzazione della Società nel suo complesso con la specificazione delle aree, strutture e uffici e relative funzioni, al fine di coordinare i conseguenti e necessari interventi sulla Parte Speciale del Modello.

Per lo svolgimento del proprio incarico, l'Organismo di Allianz Bank può, ogniqualvolta lo ritenga opportuno, disporre l'audizione dei Dirigenti, Dipendenti e Consulenti della Banca, dei responsabili di funzioni aziendali o unità

operative aziendali, nonché di qualunque altra persona, interna o esterna alla Banca, che ritenga utile convocare al fine di avere chiarimenti o approfondimenti in merito alle questioni di volta in volta analizzate. Nondimeno, l'Organismo può accedere ad ogni documento aziendale rilevante per lo svolgimento delle sue funzioni attribuite, nonché richiedere ai responsabili delle funzioni o delle unità operative aziendali informazioni, dati e/o notizie rilevanti per le sue attività di controllo.

Ad ogni modo, fermi i suoi autonomi poteri di verifica e di controllo al fine di vigilare sul funzionamento e sull'osservanza del Modello, l'Organismo di Vigilanza non ha poteri coercitivi o modificativi della struttura aziendale, né poteri di carattere sanzionatorio nei confronti dei membri degli Organi sociali, dei Dipendenti, dei Consulenti o dei *Partner*; tali poteri, infatti, rimangono riservati agli Organi sociali o alle funzioni aziendali competenti.

4.3. Le attività di *reporting* dell'Organismo di Vigilanza verso gli organi sociali

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

In particolare, l'Organismo ha tre linee di *reporting*:

i. la prima, su base **continuativa**, verso il Presidente del Consiglio di Amministratore e verso l'Amministratore Delegato;

ii. la seconda, su base **semestrale**, nei confronti del Comitato Consultivo Controlli Interni e Rischi;

iii. la terza, su base almeno **annuale**, nei confronti del Consiglio di Amministrazione. Tale relazione contiene una sintesi delle attività svolte nel corso dell'anno dall'Organismo di Vigilanza.

Qualora l'Organismo di Vigilanza rilevasse criticità riferibili a qualcuno degli organi sopraindicati, la corrispondente segnalazione è da destinarsi prontamente ad uno degli altri organi.

L'attività di *reporting* ha sempre ad oggetto: (**i**) l'attività svolta dall'Organismo di Vigilanza e (**ii**) le eventuali criticità ed i punti di miglioramento riscontrati, sia in termini di comportamenti o eventi interni ad Allianz Bank, sia in termini di efficacia del Modello.

Inoltre, l'Organismo predispone:

- **annualmente**, una relazione scritta per il Consiglio di Amministrazione contenente una sintesi di tutte le attività svolte nel corso dell'anno, dei controlli e delle verifiche eseguite, nonché l'eventuale aggiornamento della mappatura delle Attività Sensibili. In tale relazione, l'Organismo di Vigilanza predispone altresì il piano annuale delle attività previste per l'anno successivo;
- **semestralmente**, una relazione per il Comitato Consultivo Controlli Interni e Rischi descrittiva delle attività di controllo già svolte, evidenziando eventuali criticità riscontrate.

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

Il Consiglio di Amministrazione ha la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o soggetti competenti, la convocazione del predetto organo per motivi urgenti.

L'Organismo di Vigilanza deve, inoltre, coordinarsi con le competenti funzioni della Banca per i diversi profili specifici e precisamente: (**a**) con l'Unità Organizzativa Legale, ad esempio, per l'interpretazione della normativa rilevante ai fini della modifica o integrazione della mappatura delle Attività Sensibili per determinare il contenuto delle clausole contrattuali; (**b**) con l'Unità Organizzativa Segreteria Societaria per le operazioni di carattere societario ricomprese nell'elenco dei potenziali reati societari; (**c**) con la Direzione Risorse in ordine alla formazione dei Dipendenti e ad eventuali procedimenti disciplinari; (**d**) con l'Unità Organizzativa Sviluppo Professionale Risorse in ordine alla formazione dei Consulenti Finanziari abilitati all'offerta fuori sede e ad eventuali provvedimenti adottabili; (**e**) con

la funzione *Internal Audit* per il monitoraggio dei risultati dell'attività svolta ai sensi del Decreto e l'integrazione dell'attività futura; (**f**) con l'Unità Organizzativa Antiriciclaggio e Controlli Rete, a diretto riporto della Direzione *Compliance* a Antiriciclaggio in ordine al rispetto da parte dei Consulenti Finanziari abilitati all'offerta fuori sede, delle procedure amministrative e contabili aziendali nell'ambito delle Attività Sensibili; (**g**) con l'Unità Organizzativa Organizzazione, in ordine alla valutazione delle procedure interne alla Banca.

4.4. Le attività di *reporting* degli organi e delle funzioni sociali verso l'Organismo di Vigilanza

Fermo il potere dell'Organismo di Vigilanza di accedere alla documentazione societaria che dovesse ritenere opportuno analizzare per lo svolgimento del proprio incarico e della facoltà di richiedere informazioni ai responsabili delle funzioni e delle unità operative aziendali, l'Organismo deve essere comunque prontamente informato, mediante apposite segnalazioni, da parte del Consiglio di Amministrazione, dei Dipendenti e dei Consulenti Finanziari, in merito ai fatti posti in essere nell'ambito delle Attività Sensibili che potrebbero esporre la Banca al rischio di commissione di Reati.

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

- dalle funzioni che operano in aree aziendali a rischio di commissione dei Reati Presupposto ai sensi del Decreto;
- dalle funzioni di controllo;
- da altre funzioni aziendali in possesso di dati e notizie in grado di supportare l'Organismo nello svolgimento della propria attività di vigilanza;
- dagli Organi sociali e dalla società di revisione;
- dagli Organismi di Vigilanza delle altre società del Gruppo Allianz.

L'Organismo di Vigilanza può inoltre pianificare, nel proprio programma di attività annuale, incontri periodici con i responsabili delle funzioni o delle unità operative aziendali, ovvero prevederli ad evento qualora ritenuto necessario.

Ad integrazione del Modello, la Banca ha inoltre adottato la procedura «*Flussi informativi verso l'Organismo di Vigilanza*» che, *inter alia*, disciplina in dettaglio le tipologie e le tempistiche dei flussi informativi verso l'Organismo da parte di ciascuna funzione, unità operativa, Organo societario e Organismo di Vigilanza delle società del Gruppo.

4.5. Segnalazioni di fatti rilevanti all'Organismo di Vigilanza

L'Organismo di Vigilanza deve essere obbligatoriamente e prontamente informato da parte dei Destinatari del Modello in merito a eventi dai quali potrebbe scaturire, direttamente o indirettamente, addebiti di responsabilità nei confronti della Società ai sensi del D.lgs. 231/2001.

In particolare, tutti i Destinatari del Modello sono tenuti a segnalare all'Organismo (**i**) qualsiasi comportamento, tenuto nell'ambito delle attività aziendali o comunque nell'interesse della Banca, che possa configurare la commissione di un Reato ovvero la violazione delle prescrizioni del Modello o del Codice Etico e di Comportamento; e (**ii**) le informazioni indicate nel § 6.1 della procedura «*Flussi informativi verso l'Organismo di Vigilanza*».

Gli obblighi di segnalazione in capo a soggetti esterni alla Banca (come, p.e., i Consulenti), dovranno essere specificati in apposite clausole inserite nei contratti che legano tali soggetti ad Allianz Bank.

Qualora un Destinatario non adempia a tali obblighi informativi, allo stesso sarà irrogata una sanzione disciplinare che varierà a seconda della gravità dell'inottemperanza e che sarà determinata secondo le regole indicate nel capitolo 6 della Parte Generale del presente Modello. L'Organismo si riserva di segnalare agli Organi sociali o alle funzioni competenti l'opportunità di agire contro chiunque effettui in malafede segnalazioni non veritiere.

4.5.1. Contenuto e riservatezza delle segnalazioni

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

Le segnalazioni pervenute tramite i canali indicati *infra* § 4.5.2 è riservato ai soli componenti dell'Organismo di Vigilanza o a persone dagli stessi delegati.

Nel caso in cui all'Organismo pervengano segnalazioni non attinenti alla materia di cui al Decreto, lo stesso provvede a trasmetterle alle funzioni di volta in volta competenti.

4.5.2. Modalità delle segnalazioni

Coerentemente con quanto stabilito dal Codice Etico e di Comportamento, se un Dipendente desidera segnalare una violazione (o una presunta violazione) del Modello, deve riferire al suo diretto superiore. Qualora la segnalazione non dia esito, o il Dipendente si senta a disagio nel rivolgersi al suo diretto superiore per la presentazione della segnalazione, può riferire direttamente all'Organismo di Vigilanza.

I Consulenti Finanziari, per quanto riguarda la loro attività svolta nei confronti e/o per conto di Allianz Bank, effettuano la segnalazione direttamente all'Organismo di Vigilanza.

Tutte le segnalazioni all'Organismo che abbiano a oggetto l'evidenza o il sospetto della commissione – o del tentativo di commissione – di un Reato Presupposto, della violazione del Modello o del Codice Etico e di Comportamento o le altre informazioni indicate nel §6.1 della procedura «*Flussi informativi verso l'Organismo di Vigilanza*» devono essere inviate utilizzando in via prioritaria l'indirizzo di posta elettronica: OrganismodiVigilanza-231allianzbank@allianzbank.it.

L'Organismo di Vigilanza ha la facoltà di non prendere in considerazione le segnalazioni anonime che appaiano, a prima vita, irrilevanti, destituite di fondamento o non circostanziate.

L'Organismo di Vigilanza valuta le segnalazioni ricevute; gli eventuali provvedimento conseguenti sono applicati in conformità a quanto previsto nel successivo Capitolo 6 della Parte Generale del Modello.

È opportuno segnalare che anche l'*Anti-Fraud Coordinator* potrebbe ricevere segnalazioni di interesse per l'Organismo di Vigilanza: ove l'*Anti-Fraud Coordinator* dovesse ricevere tali informazioni, il medesimo inoltra – come previsto dal «*Regolamento per la gestione delle indagini su frodi interne*» e dal '*Regolamento per la gestione delle segnalazioni di casi di frode (whistleblowing procedure)*» – all'Organismo la comunicazione ricevuta e tutta la relativa documentazione allegata; tale comunicazione sarà tanto più tempestiva quanto più urgente sarà la necessità di coinvolgimento dell'Organismo di Vigilanza.

Al suddetto indirizzo di posta elettronica dovranno, quindi, essere trasmesse – oltre ai flussi informativi periodici – anche le segnalazioni indicate nel §6.1 della procedura «*Flussi informativi verso l'Organismo di Vigilanza*» e quelle inoltrate dall'*Anti Fraud Coordinator*.

La trasmissione di tutti i flussi informativi e delle segnalazioni dovrà essere corredata dai relativi documenti allegati, ove esistenti. A tal riguardo, gli Organi sociali – ove necessario – possono avvalersi della collaborazione della funzione Segreteria Societaria, la quale provvederà a trasmettere all'Organismo di Vigilanza la documentazione che possa essere utile al fine dell'analisi dei suddetti flussi.

4.5.3. Tutela del soggetto segnalante e del soggetto segnalato

Tutte le modalità di segnalazione indicate garantiscono la riservatezza dell'identità del segnalante e la tutela dei segnalanti contro qualsiasi forma di ritorsione, minaccia, discriminazione o penalizzazione.

La Banca, infatti, garantisce la tutela dei soggetti segnalanti contro qualsiasi forma, diretta o indiretta, di ritorsione, discriminazione, penalizzazione, applicazione di misure sanzionatorie, demansionamento, licenziamento, trasferimento o sottoposizione ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro per motivi collegati, direttamente o indirettamente, alla segnalazione.

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

4.6. Conservazione delle informazioni

Ogni informazione, segnalazione o documento ricevuto dall'Organismo di Vigilanza nell'adempimento del suo incarico è conservato fino a un periodo di dieci anni, nel rispetto delle previsioni di legge e secondo le modalità previste dalla procedura «*Flussi informativi verso l'Organismo di Vigilanza*».

5. Formazione e diffusione del Modello

5.1. Formazione e informazione ai Dipendenti e ai Consulenti Finanziari

Ai fini dell'efficacia del Modello, è obiettivo della Banca garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti dei Dipendenti e dei Consulenti Finanziari. Tale obiettivo riguarda tutte le risorse aziendali, sia che si tratti di risorse già presenti in azienda, sia che si tratti di quelle da inserire.

Il livello di informazione e formazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle Attività Sensibili.

Inoltre, la Banca pubblica sul sito web il proprio Modello per renderlo pienamente fruibile a tutti i Destinatari.

Il sistema di informazione e formazione è supervisionato ed eventualmente integrato dall'attività dell'Organismo, in collaborazione con il Responsabile della Direzione Risorse e con i Responsabili delle altre Direzioni/Unità Organizzative di volta in volta coinvolti nell'applicazione del Modello.

5.1.1. La comunicazione iniziale

Ad ogni nuovo assunto e a coloro ai quali è stato conferito per la prima volta un mandato di Consulente Finanziario viene consegnato un *set* informativo, con il quale assicurare le conoscenze di primaria rilevanza. Tale *set* informativo dovrà contenere, tra l'altro, il Codice Etico e di Comportamento ed il Modello.

Tali soggetti saranno tenuti a rilasciare alla Banca una dichiarazione firmata ove si attesti di aver ricevuto il *set* informativo, l'integrale conoscenza dei documenti ricevuti, nonché per i Dipendenti, l'impegno a osservarne le prescrizioni.

5.1.2. La formazione

L'attività di formazione è finalizzata a diffondere la conoscenza della normativa di cui al D.lgs. 231/2001 ed è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano e dal fatto che gli stessi abbiano o meno funzioni di rappresentanza della Banca.

In particolare, la Banca ha previsto livelli diversi di formazione attraverso idonei strumenti di diffusione per:

a) i Dipendenti della Banca che rivestono la qualifica di Dirigenti;

b) i Dipendenti della Banca che non rivestono la qualifica di Dirigenti e i Consulenti Finanziari;

c) i membri del Consiglio di Amministrazione e del Collegio Sindacale.

Le modalità di espletamento dell'attività formativa sono sottoposte a costanti verifiche di adeguatezza da parte dell'Organismo di Vigilanza, il quale, ove necessario, provvede a modificarle.

La mancata partecipazione non giustificata ai programmi di formazione costituisce un illecito disciplinare.

5.1.3. Le comunicazioni successive

L'Organismo di Vigilanza, in coordinamento con le altre competenti funzioni aziendali, curerà le comunicazioni successive ai Destinatari del Modello che si renderanno eventualmente necessarie a fronte degli interventi di aggiornamento e modifica dello stesso.

È comunque compito delle competenti funzioni aziendali verificare che sul sito *internet* della Banca sia pubblicata la versione più aggiornata del Modello e del Codice Etico e di Comportamento.

5.2. Informazioni alle Società di Service

Le Società di Service sono informate dell'avvenuta adozione del Modello e dell'esigenza per Allianz Bank che il loro comportamento sia conforme ai disposti del D.lgs. 231/2001, nonché a quelli del Codice Etico e di Comportamento della Banca.

5.3. Informazioni ai Consulenti, Fornitori e *Partner*

Relativamente ai Consulenti, ai Fornitori e ai *Partner*, a cura delle competenti Direzioni/Unità Organizzative, sono istituiti appositi sistemi di valutazione per la selezione dei medesimi e di informativa nei loro confronti.

In ogni caso, nei contratti con Consulenti, Fornitori e *Partner* dovranno essere inserite specifiche clausole con cui gli stessi si obbligano al rispetto dei principi dettati dal d.lgs. 231/2001 e secondo quanto previsto nel Modello.

6. Sistema sanzionatorio

6.1. Principi generali

La definizione di un sistema di sanzioni disciplinari applicabili in caso di violazione delle regole di cui al presente Modello rende efficiente l'azione di vigilanza dell'Organismo e ha lo scopo di garantire l'effettività del Modello stesso.

La definizione di tale sistema sanzionatorio, infatti, costituisce ai sensi dell'art. 6, co. 1, lett. e), D.lgs. 231/2001 un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità della Banca. Inoltre, ai sensi della L. 179/2017 in materia di *whistleblowing*, il legislatore italiano ha stabilito che, nel suddetto sistema disciplinare, devono essere espressamente previste «*sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate*» (art. 6, co. 2-*bis*, lett. d), D.lgs. 231/2001).

Ulteriore presupposto per l'effettività del Modello è che ogni ipotesi di violazione sia portata all'attenzione dell'Organismo di Vigilanza e riceva un adeguato seguito. A tale scopo, la Banca ha adottato la procedura «*Flussi informativi verso l'Organismo di Vigilanza*» che ha, tra l'altro, l'obiettivo di assicurare tempestivo, approfondito e imparziale svolgimento di idonei accertamenti sulla segnalazione pervenuta, al fine di dare a esse soddisfacente seguito.

Ad ogni modo, l'applicazione delle misure sanzionatorie di seguito richiamate non pregiudica né modifica ulteriori ed eventuali conseguenze civilistiche o di altra natura (p.e., penale, amministrativa o tributaria), che possano derivare dal medesimo fatto.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale avviato dall'Autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche a integrare un Reato Presupposto; le regole di condotta sono infatti assunte dall'azienda in piena autonomia e indipendentemente dall'illecito penale che eventuali condotte possano determinare: il sistema disciplinare non solo è autonomo rispetto all'eventuale azione penale esercitata dall'Autorità giudiziaria o di un procedimento iniziato da una Autorità amministrativa indipendente, ma invero deve rimanere su un piano nettamente distinto e separato dal sistema normativo del diritto penale e di quello amministrativo.

Nel caso in cui la Banca preferisca comunque attendere l'esito del giudizio penale (o del procedimento amministrativo), essa potrà ricorrere all'istituto dell'allontanamento temporaneo dal servizio e rinviare alle risultanze anche non definitive del giudizio penale (o del procedimento amministrativo) l'eventuale avvio di un procedimento disciplinare.

A seguito dell'avvio di un procedimento disciplinare da parte delle funzioni aziendali competenti, l'Organismo di Vigilanza deve essere prontamente informato circa l'eventuale applicazione di una sanzione per una violazione del Modello (o delle procedure adottate dalla Banca per la sua attuazione) e del Codice Etico e di Comportamento, disposta nei confronti di qualsivoglia soggetto tenuto all'osservanza degli stessi.

Infine, con riferimento al sistema sanzionatorio relativo alla corretta gestione delle segnalazioni di illeciti ai sensi dell'art. 6, co. 2-*bis*, D.lgs. 231/2001, nei confronti di tutti i Destinatari del Modello sono previste (**i**) sanzioni per chi pone in essere atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di un soggetto che abbia effettuato la segnalazione per motivi collegati, direttamente o indirettamente, alla segnalazione stessa; (**ii**) sanzioni nei confronti di chi effettua, con dolo o colpa grave, segnalazioni che si rivelano infondate. Le misure di carattere disciplinare sono definite in relazione al ruolo del destinatario delle stesse secondo quanto indicato nei paragrafi successivi, poiché la violazione delle norme relative al sistema di segnalazione di fatti illeciti o rilevanti rappresenta, a tutto gli effetti, un'inosservanza del Modello.

6.2. Misure nei confronti dei Dipendenti e dei Consulenti Finanziari

La violazione da parte dei Dipendenti della Società a cui si applica il CCNL delle singole regole comportamentali di cui al presente modello costituisce illecito disciplinare. I provvedimenti applicabili, in particolare, variano a seconda che il Dipendente rivesta o meno anche la qualifica di Dirigente.

6.2.1. Dipendenti che non rivestono la qualifica di Dirigente

I provvedimenti disciplinari irrogabili nei confronti dei Dipendenti che non rivestono la qualifica di Dirigente – nel rispetto delle procedure previste dall'art. 7 della legge 30 maggio 1970, n. 300 e delle eventuali norme speciali applicabili – sono quelli previsti dall'apparato sanzionatorio di cui al CCNL applicabile alla Banca. Più precisamente:

- il **rimprovero verbale**;
- il **biasimo scritto**;
- la **sospensione dal servizio e dal trattamento economico**;
- il **licenziamento per giustificato motivo**;
- il **licenziamento per giusta causa**.

Restano ferme – e si intendono qui a tutti gli effetti richiamate – tutte le disposizioni previste dalla legge e dal CCNL applicati, relative alle procedure e agli obblighi da osservare nell'applicazione delle sanzioni disciplinari. Inoltre, per quanto riguarda l'accertamento delle violazioni, il procedimento disciplinare e l'irrogazione della sanzione disciplinare, restano invariati i poteri già conferiti, nei limiti delle rispettive attribuzioni, agli organi e funzioni aziendali competenti.

Nello specifico, i comportamenti che costituiscono un illecito disciplinare sono:

a) il compimento, nell'espletamento di una delle Attività Sensibili o, comunque, di un attività nell'interesse della Banca o che potrebbe determinare un vantaggio diretto o indiretto alla stessa, di comportamenti in violazione delle prescrizioni del Modello e del Codice Etico e di Comportamento, tali da poter determinare la concreta applicazione a carico della Banca di sanzioni previste dal D.lgs. 231/2001;

b) la violazione delle procedure adottate e richiamate dal presente Modello o, comunque, il compimento, nell'espletamento di una delle Attività Sensibili o di un'altra attività compiuta nell'interesse della Banca o che potrebbe determinare un vantaggio diretto o indiretto alla stessa, di comportamenti non conformi alle prescrizioni del Modello o del Codice Etico e di Comportamento, a prescindere dal fatto che da tali possano o meno derivare sanzioni per la Banca ai sensi del D.lgs. 231/2001;

c) il compimento di atti di ritorsione o di atti discriminatori, diretti o i diretti, nei confronti di un soggetto che abbia effettuato una segnalazione di una possibile violazione del Modello, del Codice Etico e di Comportamento, delle procedure adottate dalla Banca e richiamate nel presente Modello o comunque abbia segnalato una delle altre informazioni elencate nel §6.1 della procedura «*Flussi informativi verso l'Organismo di Vigilanza*» per motivi collegati, direttamente o indirettamente, alla segnalazione stessa;

d) il compimento, con dolo o colpa grave, di una segnalazione infondata di una possibile violazione del Modello, del Codice Etico e di Comportamento, delle procedure adottate dalla Banca e richiamate nel presente Modello o delle altre informazioni elencate nel §6.1 della procedura «*Flussi informativi verso l'Organismo di Vigilanza*».

6.2.2. Dipendenti che rivestono la qualifica di Dirigente

Nell'ipotesi in cui fosse un Dirigente a (**i**) compiere, nell'espletamento di una delle Attività Sensibili o, comunque, di un attività nell'interesse della Banca o che potrebbe determinare un vantaggio diretto o indiretto alla stessa, comportamenti in violazione delle prescrizioni del Modello, del Codice Etico e di Comportamento o delle procedure

adottate dalla Società e richiamate nel Modello, (**ii**) compiere atti di ritorsione o di atti discriminatori, diretti o i diretti, nei confronti di un soggetto che abbia effettuato una segnalazione, ovvero (**iii**) compiere, con dolo o colpa grave, una segnalazione infondata, la Banca provvederà ad applicare le misure più idonee in conformità a quanto previsto dalla normativa di riferimento.

Per quanto riguarda l'accertamento delle violazioni, il procedimento disciplinare e l'irrogazione della sanzione disciplinare, restano invariati i poteri già conferiti, nei limiti delle rispettive attribuzioni, agli organi e funzioni aziendali competenti.

Si precisa infine che, in base a specifico regolamento di Allianz Bank, le suddette violazioni o non conformità incidono negativamente sulla valutazione alla base della quantificazione del premio annuale ovvero sui risultati di cui ai programmi di *Management by Objectives* con conseguente riduzione del compenso variabile.

Anche in questo caso, restano ferme – e si intendono qui a tutti gli effetti richiamate – tutte le disposizioni previste dalla legge e dal CCNL applicati dalla Banca relative alle procedure e agli obblighi da osservare nell'applicazione delle sanzioni disciplinari.

6.2.3. Disposizioni comuni

Il sistema sanzionatorio è soggetto a costante verifica e valutazione da parte dell'Organismo e del Responsabile dell'Unità Organizzativa Risorse Umane, rimanendo quest'ultimo il soggetto incaricato della concreta applicazione delle misure disciplinari sopra richiamate.

Rimane comunque salvo il diritto al risarcimento di ogni danno arrecato alla Banca.

Più specificamente, il tipo e l'entità di ciascuna delle sanzioni richiamate, nonché l'eventuale richiesta di risarcimento del danno da parte della Banca, saranno applicate in relazione:

- alle mansioni, al livello di responsabilità e di autonomia del Dipendente o del Dirigente;
- all'intenzionalità del comportamento o al grado di negligenza, imprudenza o imperizia;
- al comportamento complessivo del Dipendente o del Dirigente, con particolare riguardo, nei limiti consentiti dalla legge, alla sussistenza di precedenti disciplinari a carico del medesimo;
- alle particolari circostanze che accompagnano la violazione disciplinare.

6.2.4. Consulenti Finanziari abilitati all'offerta fuori sede

Le caratteristiche proprie dell'attività di Consulente Finanziario, così come definita dalla vigente normativa applicabile in termini di obblighi e regole di comportamento, prevedono altresì l'impegno, per ogni Consulente Finanziario abilitato all'offerta fuori sede, di rispettare le procedure ed i codici di comportamento del soggetto che ha conferito l'incarico.

In particolare, a titolo esemplificativo, costituiscono comportamenti sanzionabili con connotazione di gravità crescente: (**i**) la violazione delle procedure previste dal Modello o l'adozione di comportamenti non conformi al Modello nell'espletamento delle Attività Sensibili; (ii) violazioni dello stesso tipo che espongono la Banca ad una situazione oggettiva di rischio imminente di commissione di uno o più Reati; (iii) adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello e univocamente diretti al compimento di uno o più Reati, ovvero di comportamenti in palese violazione del Modello, tali da determinare la concreta applicazione delle sanzioni previste dal Decreto.

Le sanzioni saranno commisurate (**i**) all'intenzionalità del comportamento del Consulente Finanziario abilitato all'offerta fuori sede, (**ii**) alla gravità del comportamento, nonché (**iii**) all'eventuale esistenza di precedenti violazioni del Modello commesse dallo stesso Consulente Finanziario abilitato all'offerta fuori sede.

Sono previste le seguenti misure sanzionatorie:

- **censura scritta** con richiamo al rigoroso rispetto delle disposizioni del presente Modello;
- **sospensione temporanea** dall'attività di Consulente Finanziario;
- **recesso per giusta causa**.

Per quanto riguarda l'accertamento delle violazioni la competenza è riservata ai Responsabili di Direzione e dell'Unità Organizzativa a ciò deputate.

In ogni caso, resta fermo il risarcimento dei danni eventualmente derivati alla Banca dal comportamento del Consulente Finanziario abilitato all'offerta fuori sede.

6.3. Misure nei confronti degli amministratori

In caso di violazioni del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa l'intero Consiglio di Amministrazione, affinché possa prendere gli opportuni provvedimenti, tra i quali, per esempio, la convocazione dell'Assemblea dei Soci al fine di adottare le misure più idonee previste dalla legge e/o la revoca di deleghe eventualmente conferite all'amministratore, ovvero la necessaria comunicazione alla Banca d'Italia.

6.4. Misure nei confronti dei sindaci

In caso di violazione del Modello da parte di uno o più Sindaci, uno dei membri dell'Organismo di Vigilanza informa il Consiglio di Amministrazione affinché possa effettuare necessarie verifiche ed assumere opportuni provvedimenti.

6.5. Misure nei confronti delle Società di Service, Consulenti, Fornitori e *Partner*

Ogni comportamento posto in essere dalle Società di Service, dai Consulenti, dai Fornitori o dai *Partner* in violazione della normativa di cui al Decreto, nonché ogni commissione dei Reati, è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti, ovvero secondo quanto appositamente comunicato in merito.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Banca, come nel caso di applicazione alla stessa da parte del Giudice delle misure previste dal Decreto.

7. Introduzione alla Parte Speciale

7.1. Principi generali

In conformità all'art. 6 del Decreto, il sistema dei controlli interni di un ente, in relazione ai Reati da prevenire, deve, tra le altre cose, prevedere: (**i**) l'individuazione delle attività nel cui ambito possano essere commessi gli illeciti; (**ii**) specifici protocolli per programmare la formazione e l'attuazione delle decisioni dell'ente; (**iii**) l'individuazione delle modalità di gestione delle risorse finanziarie idonee a prevenire la commissione degli illeciti.

Anche a tale scopo, la Parte Speciale del Modello ha la finalità di definire le linee di condotta e le regole di comportamento che devono essere seguite al fine di prevenire, nell'ambito delle Attività Sensibili rilevate presso Allianz Bank la possibile commissione di taluno dei Reati Presupposto e, prima ancora, di assicurare l'integrità e la trasparenza nello svolgimento delle attività della Società.

La Parte Speciale del Modello ha altresì lo scopo di fornire all'Organismo di Vigilanza gli strumenti per esercitare le attività di monitoraggio, controllo e verifica sulle Aree Sensibili individuate.

La Parte Speciale, in particolare, disciplina:

i. l'attività di chiunque operi per conto della Banca in forza di un rapporto di lavoro dipendente, dell'assunzione di incarichi di gestione o controllo della Società, o di un qualsiasi altro legame che lo sottoponga alla direzione dei Soggetti Apicali della Società;

ii. nei limiti delle disposizioni applicabili, l'attività di chiunque, pur non essendo uno dei soggetti individuati *sub* i), operi nel suo interesse in forza di rapporti contrattuali.

Sono ammesse, nei casi di particolare urgenza o in caso di impossibilità temporanea e comunque sotto la responsabilità di chi le attua, eventuali deroghe a quanto previsto nella Parte Speciale del Modello. In tale evenienza, tuttavia, deve essere inviata immediata informazione all'Organismo di Vigilanza e, in ogni caso, è richiesta la successiva ratifica della decisione da parte del soggetto di volta in volta competente.

In linea generale, il sistema di organizzazione della Banca deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, di rappresentanza e di definizione delle linee gerarchiche e delle attività operative.

Ad ogni modo, tutte le Attività Sensibili devono essere svolte conformandosi alla legge, alle previsioni del Codice Etico e di Comportamento, alle regole contenute nel Modello e alle procedure adottate dalla Banca.

7.2. La documentazione interna di Allianz Bank

La documentazione interna (*e.g.*, funzionigrammi, procedure, comunicazioni organizzative, ecc.) richiamata dalla Parte Speciale del Modello devono intendersi parte integrante dello stesso.

Più in generale, la documentazione interna della Banca è caratterizzata dai seguenti principi: (**i**) conoscibilità all'interno della Banca (e, ove necessario, anche nei confronti delle altre società del Gruppo bancario); (**ii**) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri; (**iii**) chiara descrizione delle linee di riporto.

Le procedure interne di Allianz Bank, in particolare, devono inoltre prevedere i seguenti elementi: (**i**) massima separatezza, all'interno di ciascun processo, tra il soggetto che lo inizia, il soggetto che lo esegue e/o lo conclude e il soggetto che lo controlla; (**ii**) tracciabilità scritta di ciascun passaggio rilevante del processo; (**iii**) adeguato livello di formalizzazione; (**iv**) divieto di prevedere sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna basati su *target* di *performance* sostanzialmente irraggiungibili.

Le procedure adottate dalla Banca richiamate dalla Parte Speciale del Modello sono costantemente aggiornate dagli organi competenti, anche su proposta dell'Organismo di Vigilanza.

È infatti compito dell'Organismo vigilare che le procedure siano idonee al rispetto dei principi contenuti nel Modello.

7.3. Il sistema di deleghe e procure di Allianz Bank

In linea generale, deve intendersi per **delega** quell'atto interno alla Banca di attribuzione di funzioni e compiti riflesso nel sistema di comunicazioni organizzative. Viceversa, deve intendersi per **procura** il negozio giuridico unilaterale con cui la Banca attribuisce dei poteri di rappresentanza nei confronti di soggetti terzi. Di riflesso, all'interno della Banca, ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza, viene conferita una *procura generale funzionale* di estensione adeguata e coerente con le funzioni e i poteri di gestione attribuiti al titolare attraverso la *delega*.

Il sistema di deleghe e procure, in linea di principio, deve essere caratterizzato da elementi che assicurino la prevenzione dei Reati Presupposto e, nel contempo, consentano comunque la gestione efficiente dell'attività aziendale.

Per tale ragione, nell'ambito delle attività della Banca, i requisiti essenziali del sistema di deleghe sono:

a) l'obbligo, per tutti coloro – compresi anche i dipendenti o gli organi sociali di altre società del Gruppo bancario e delle Società di Service– che intrattengono per conto di Allianz Bank rapporti con la Pubblica Amministrazione, di essere dotati di delega formale in tal senso;

b) le necessità di coniugare ciascun potere di gestione alla relativa responsabilità e a una posizione adeguata nell'organigramma aziendale, nonché quella di aggiornare il sistema a seguito di mutamenti organizzativi;

c) la necessità per ciascuna delega di definire in modo specifico e univoco sia i poteri del delegato, sia il soggetto (organo aziendale o individuo) cui il delegato riporta gerarchicamente;

d) le coerenza tra i poteri gestionali assegnati con la delega e gli obiettivi aziendali;

e) la disponibilità di poteri di spesa adeguati alle funzioni conferite con la delega.

Invece, i requisiti essenziali del sistema di attribuzione delle procure, sono:

a) le procure generali funzionali, sono conferite esclusivamente ai soggetti dotati di delega interna, o relativamente ai Consulenti finanziari parti di specifico contratto di incarico di promozione finanziaria;

b) le procure generali descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione aziendale che fissi l'estensione di poteri di rappresentanza ed i limiti di spesa numerici;

c) la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;

d) una procedura *ad hoc* deve disciplinare modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le procure devono essere attribuite, modificate e revocate (a causa, per esempio, dell'assunzione o estensione di nuove responsabilità e poteri, del trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, di dimissioni, licenziamento e revoca, ecc.).

L'Organismo di Vigilanza verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la coerenza con tutto il sistema delle comunicazioni organizzative (*e.g.*, i documenti interni alla Banca con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

PARTE SPECIALE

1. Reati nei rapporti con la Pubblica Amministrazione

1.1. Le fattispecie di reato rilevanti di cui all'art. 24, D.lgs. 231/2001

MALVERSAZIONE A DANNO DELLO STATO (ART. 316-*BIS* C.P.)

Tale reato si configura quando, dopo aver ricevuto finanziamenti, sovvenzioni o contributi da parte dello Stato, di altro ente pubblico o dell'Unione europea, destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate.

La condotta illecita consiste appunto nella distrazione, anche parziale, della somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta. Non rileva neppure l'eventuale destinazione delle somme ottenute a una finalità di pubblico interesse diversa da quella sottostante all'erogazione, rientrante o meno nell'oggetto sociale del beneficiario; non rileva, ancora, neanche che tale finalità diversa risulti ugualmente utile.

Nel caso in cui sia previsto esplicitamente o implicitamente un termine finale essenziale per la realizzazione dell'opera, costituisce reato la violazione dello stesso e il conseguente ritardo di dimensioni tali da incidere sul soddisfacimento degli interessi pubblici connessi alla realizzazione dell'opera. Tenuto conto che il momento consumativo di questo reato coincide con la fase esecutiva, inoltre, l'illecito può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

Esempio

I Dipendenti della Banca, cui è stata affidata la gestione di un finanziamento pubblico per scopi di formazione del personale, utilizzano i fondi per l'acquisto di dispositivi elettronici.

Un Dipendente della Banca, d'accordo con il cliente e pertanto in concorso con lo stesso, approva un finanziamento garantito da Sace S.p.A. di cui al D.L. 8 aprile 2020, n. 23 (conv. con modificazioni dalla L. 5 giugno 2020, n. 40) a favore di una società del cliente, consapevole che la stessa lo utilizzerà per investimenti esteri.

INDEBITA PERCEZIONE DI CONTRIBUTI, FINANZIAMENTI O EROGAZIONI DA PARTE DELLO STATO (ART. 316-*TER* C.P.)

Tale ipotesi di reato si configura nei casi in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere o mediante l'omissione di informazioni dovute, si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dell'Unione europea. A differenza dell'ipotesi di malversazione descritta in precedenza, in questo caso a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato si realizza nel momento dell'ottenimento dei finanziamenti.

Va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie di truffa ai danni dello Stato: essa trova, infatti, applicazione essenzialmente laddove l'erogazione non sia l'effetto dell'induzione in errore dell'ente erogante.

Esempi

Un Dipendente della Banca rilascia a un cliente una garanzia fideiussoria fittizia per consentirgli di ottenere un finanziamento pubblico.

Un Dipendente della Banca, d'accordo con il cliente e pertanto in concorso con lo stesso, approva un finanziamento garantito da Sace S.p.A. di cui al D.L. 8 aprile 2020, n. 23 (conv. con modificazioni dalla L. 5 giugno 2020, n. 40) a favore di una società del cliente, consapevole che il rappresentante legale della stessa ha falsamente dichiarato di non rientrare nella categoria delle imprese in difficoltà.

La Banca consegue un finanziamento da parte dello Stato per l'assunzione di personale appartenente a categorie protette, producendo dichiarazioni non rispondenti al vero come, p.e., l'indicazione di un numero di Dipendenti superiore rispetto a quello effettivamente impiegato.

TRUFFA A DANNO DELLO STATO O DI UN ALTRO ENTE PUBBLICO (ART. 640, CO. 2, C.P.)

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

Nella nozione di *artifici* – *i.e.*, l'alterazione della realtà esteriore che si realizza simulando l'inesistente o dissimulando l'esistente – o *raggiri* – che, essenzialmente, consistono in una menzogna qualificata perché corredata da ragionamenti e discorsi tali da farla recepire come veritiera – sono compresi anche la menzogna o il silenzio maliziosamente serbato su alcune circostanze rilevanti ai fini della conclusione del contratto, quando abbiano determinato l'errore altrui, inducendo il soggetto ingannato a compiere un atto di disposizione patrimoniale dal quale sia conseguito un ingiusto profitto a favore dell'autore del reato, con altrui danno. Inoltre, ai fini della sussistenza della truffa ai danni dello Stato o di altro ente pubblico, è necessario che lo Stato o altro ente pubblico patisca il danno patrimoniale, mentre non è indispensabile che il soggetto ingannato rivesta una funzione pubblica (si pensi, p.e., all'inganno ai danni di un funzionario di banca che sia indotto a trasferire denaro al truffatore denaro di un ente pubblico). Il profitto, ancora, può consistere anche in una mancata diminuzione patrimoniale o in altro vantaggio.

Nella nozione di *ente pubblico*, rientra qualsiasi ente che persegua finalità pubbliche o svolga funzioni di preminente interesse pubblico. Rileva, infine, precisare che la giurisprudenza ha spesso catalogato come enti pubblici anche i soggetti di diritto privato che siano concessionari di pubblici servizi, nonché le società che siano partecipate a maggioranza da un ente pubblico.

Esempio

Nella predisposizione di documenti per la partecipazione a una procedura di gara, un Dipendente della Banca fornisce alla Pubblica Amministrazione informazioni non veritiere – perché, p.e., supportate da documentazione artefatta – così ottenendo l'aggiudicazione della gara stessa.

TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640-*BIS* C.P.)

Il reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche da parte dello Stato, di enti pubblici o dell'Unione europea.

La fattispecie illecita può realizzarsi nel caso in cui si pongano in essere artifici o raggiri quali possono essere il comunicare dati non veritieri o il predisporre documentazione falsa per ottenere i finanziamenti pubblici.

Esempio

Un Dipendente della Banca, d'accordo con un cliente e pertanto in concorso con lo stesso, predispone documentazione artefatta grazie alla quale il cliente ottiene indebitamente un contributo o un finanziamento pubblico.

FRODE INFORMATICA A DANNO DELLO STATO O DI UN ALTRO ENTE PUBBLICO (ART. 640-*TER* C.P.)

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

Esempio

Un Dipendente della Banca altera i software utilizzati per le segnalazioni di vigilanza o le denunce redditi così realizzando un ingiusto profitto in favore della Banca con danno in capo all'ente stesso.

1.2. Le fattispecie di reato rilevanti di cui all'art. 25, D.lgs. 231/2001

CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE (ART. 318 C.P.)

CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI D'UFFICIO (ART. 319 C.P.)

Il reato di corruzione consiste in un accordo tra un pubblico ufficiale e un soggetto 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 c.d. *propria*) ovvero per l'esercizio, ancorché conforme ai suoi doveri, della sua funzione o dei suoi poteri, a prescindere dall'effettivo compimento di uno specifico atto (corruzione c.d. *impropria*).

Nella corruzione *impropria ex* art. **318** c.p., l'attività del pubblico ufficiale è pienamente conforme all'interesse pubblico e ciò che si intende punire è esclusivamente il mercimonio della funzione. Nel caso della corruzione *propria ex* art. **319** c.p., invece, il pubblico ufficiale accetta una retribuzione in cambio di un atto contrario ai suoi doveri, oppure in cambio dell'asservimento della pubblica funzione agli interessi del privato.

Nei delitti di corruzione, il pubblico ufficiale e il privato si pongono in posizione paritaria, diversamente dalla concussione (art. 317 c.p.) che, invece, presuppone lo sfruttamento da parte del funzionario della propria posizione di superiorità, alla quale corrisponde una situazione di soggezione nel privato. Per tale ragione, nei delitti di corruzione, sia il corrotto sia il corruttore sono puniti, a differenza di quanto avviene invece nella concussione, che punisce invece solo il pubblico ufficiale proprio in considerazione della situazione di squilibrio che si instaura tra i soggetti.

Ai sensi dell'art- **319-*bis*** c.p. («*Circostanze aggravanti*»), la pena del delitto di corruzione *propria* è aumentata se il fatto di cui all'art. 319 c.p. ha per oggetto il conferimento di pubblichi impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene, nonché il pagamento o il rimborso di tributi.

Si noti, inoltre, che l'art. **320** c.p. estende l'applicabilità di entrambe le fattispecie agli incaricati di un pubblico servizio.

È l'art. **321** c.p., invece, a stabilire che le pene di cui agli artt. 318, 319, 319-*bis*, 319-*ter* («*Corruzione in atti giudiziari*», di cui si dirà *infra*) e 320 c.p. si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di pubblico servizio denaro o altra utilità.

Esempi

Un Dirigente della Banca offre una somma di denaro a un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo per l'esercizio dell'attività della Banca.

Un Dipendente della Banca, affinché il pubblico ufficiale agevoli indebitamente la Banca nell'esercizio delle sue funzioni (i) stipula contratti per l'acquisto di beni o servizi (p.e., arredamento, hardware, software, pubblicità, materiali di marketing, consulenze, ecc.) con i fornitori suggeriti dal pubblico ufficiale e a questi legati direttamente o indirettamente a importi superiori al valore reale del bene o del servizio ovvero ai prezzi di mercato; (ii) paga compensi a professionisti legati direttamente o indirettamente al pubblico ufficiale relativi a consulenze in realtà non rese; (iii) paga fatture a fornitori suggeriti dal pubblico ufficiale e a questi legati direttamente o indirettamente relative ad acquisti di beni mai realizzati ovvero alla retribuzione di servizi mai effettuati; (iii) predispone budget di spesa non veritieri e retrocede i danari al pubblico ufficiale; (iv) dà o promette al pubblico ufficiale, che accetta la dazione o la promessa, regali o omaggi che esulano dalle normali pratiche commerciali; (v) assume alle dipendenze della Banca persona segnalata dal pubblico ufficiale ovvero seleziona promotori e collaboratori da quest'ultimo indicati, nel mancato rispetto delle procedure aziendali vigenti in materia o in assenza delle qualifiche richieste dal ruolo; ovvero, ancora, (vi) riconosce al pubblico ufficiale condizioni particolarmente favorevoli alle condizioni standard applicabili a operazioni bancarie simili.

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

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

Esempi

Un Dirigente della Banca versa denaro a un cancelliere del Tribunale affinché accetti, seppur fuori termine, delle memorie difensive o delle produzioni documentali, consentendo quindi di superare i limiti temporali previsti dai codici di procedura a tutto vantaggio della propria difesa.

Un Dirigente della Banca dà o promette denaro o altra utilità a un magistrato, cancelliere o altro funzionario per assicurarsi il positivo esito di un processo civile, penale o amministrativo.

Un Dirigente della Banca dà denaro a un professionista di fiducia affinché quest'ultimo ricompensi un magistrato, cancelliere o altro funzionario al fine di assicurarsi il positivo esito di un processo civile, penale o amministrativo.

Un Dirigente della Banca dà o promette denaro o altra utilità a un magistrato o altro soggetto affinché quest'ultimo intervenga presso altri magistrati colleghi o altri soggetti ritenuti idonei a incidere in senso favorevole alla Società in relazione a vicende processuali di cui è parte o ha un interesse.

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

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

A differenza di quanto avviene per la concussione (art. 317 c.p.), in questo caso è punibile anche il soggetto che, per effetto delle pressioni subite, è indotto alla promessa o dazione di utilità. Si ritiene, infatti, che la minor intensità delle pressioni – di qui la differenza tra costrizione e induzione – consenta comunque al privato di non accedere alla richiesta.

Esempio

Un Dirigente della Banca, nell'ambito di conversazioni telefoniche intercorrenti con un funzionario di Banca d'Italia in occasione di una visita ispettiva, viene indotto dal suddetto funzionario ad assumere il proprio figlio in Banca per evitare controlli più stringenti.

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

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

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

Esempio

Un Dirigente della Banca offre una somma di denaro a un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo per l'esercizio dell'attività della Banca ma il pubblico ufficiale rifiuta l'offerta.

PECULATO, CONCUSSIONE, CORRUZIONE E ISTIGAZIONE ALLA CORRUZIONE DI MEMBRI DEGLI ORGANI DELLE COMUNITÀ EUROPEE E DI FUNZIONARI DELLE COMUNITÀ EUROPEE E DI STATI ESTERI (ART. 322-*BIS* C.P.)

Ai sensi dell'art. 322-*bis* , co. 1, c.p. le disposizioni del codice penale in tema di corruzione, corruzione in atti giudiziari, induzione indebita a dare o promettere utilità e istigazione alla corruzione si applicano anche quando i soggetti che svolgono funzioni pubbliche sono (**i**) membri della Commissione europea, del Parlamento europeo, della Corte di Giustizia e della Corte dei Conti dell'Unione europea; (**ii**) funzionari e agenti assunti per contratto a norma dello statuto dei funzionari dell'Unione europea o del regime applicabile agli agenti dell'Unione europea; (**iii**) persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso l'Unione europea, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti dell'Unione europea; (**iv**) membri e addetti a enti costituiti sulla base dei Trattati che istituiscono l'Unione europea; (**v**) coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio; (**vi**) giudici, procuratori, procuratori aggiunti, funzionari e agenti della Corte penale internazionale, persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, membri e addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale; (**vii**) persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali; (**viii**) 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.

Inoltre, ai sensi dell'art. 322-*bis*, co. 2, c.p., nell'ipotesi di induzione indebita a dare o promettere utilità (319-*quater*, co. 2, c.p.), nelle ipotesi di corruzione (art. 321 c.p.) e di istigazione alla corruzione (art. 322, co. 1 e 2, c.p.), il soggetto privato è punito quando il denaro o altra utilità è dato, offerto o promesso (**i**) alle persone indicate dall'art. 322-*bis*, co. 1, c.p. e sopra richiamate; (**ii**) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

Esempio

Un Dirigente della Banca dà o promette denaro o altra utilità a un funzionario della Banca Centrale Europea affinché lo stesso blocchi un procedimento ispettivo nei confronti della Banca.

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

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

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

Si noti, inoltre, che il comma 4 della medesima disposizione prevede un innalzamento del trattamento sanzionatorio se «*i fatti sono commessi in relazione all'esercizio di attività giudiziarie*».

Esempio

Un Dipendente della Banca accetta di corrispondere una somma di denaro a Tizio, il quale, vantando asserite conoscenze o "entrature" con esponenti della Banca d'Italia, si offre di "intercedere" presso di loro, al fine di ottenere la chiusura senza rilievi di una procedura ispettiva che, in realtà, ha ravvisato violazioni procedurali meritevoli di sanzioni da parte della Banca d'Italia nei confronti delle Società.

1.3. Processi e attività sensibili rilevanti

In relazione ai Reati nei rapporti con la Pubblica Amministrazione sino a qui descritti, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti – soprattutto perché comportano un contatto, diretto o indiretto, degli esponenti della Società con soggetti appartenenti alla Pubblica Amministrazione – sono i seguenti:

I. Gestione degli adempimenti e dei rapporti con gli enti pubblici e le autorità amministrative indipendenti, anche in occasione di verifiche ispettive;

II. Gestione dei flussi monetari e finanziari;

III. Selezione e gestione dei consulenti finanziari;

IV. Formazione del bilancio e gestione degli adempimenti societari e dei rapporti con gli organi di controllo;

VI. Gestione dell'erogazione del credito;

VII. Acquisto di beni, servizi e consulenze;

VIII. Selezione, assunzione e gestione del personale;

IX. Gestione di omaggi, delle sponsorizzazioni e altre liberalità;

X. Gestione del contenzioso;

XI. Utilizzo dei sistemi informatici aziendali.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Negoziazione, stipula ed esecuzione di contratti con enti pubblici di rilevanza nazionale e internazionale, con particolare riferimento alla gestione dei rapporti con pubblici ufficiali in fase di: (**i**) predisposizione della documentazione di offerta; (**ii**) definizione e stipula del contratto; (**iii**) esecuzione e rendicontazione delle attività, nonché gestione degli aspetti amministrativi e dei creditori connessi

- Processo Sensibile principale: **I**

b) Gestione degli adempimenti e dei rapporti con le Autorità Pubbliche di vigilanza (*e.g.*, CONSOB, Banca d'Italia ecc.) in occasione di verifiche, ispezioni e accertamenti

- Processo Sensibile principale: **I**

c) Gestione degli adempimenti e dei rapporti nei confronti dei funzionari della Guardia di Finanza, Agenzia delle Entrate, Camera di Commercio, Industria e Artigianato, Ufficio del Registro, Tribunale e altri enti competenti in materia fiscale, tributaria e societaria, nonché con le Autorità di pubblica sicurezza anche in occasione di verifiche, ispezioni, accertamenti e gestione delle relative comunicazioni

- Processi Sensibili principali: **I** e **IV**

d) Gestione degli adempimenti e dei rapporti nei confronti dei funzionari dell'Istituto Nazionale della Previdenza Sociale, dell'Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro, dell'Azienda Sanitaria Locale, dell'Ispettorato del Lavoro e della Direzione Provinciale del Lavoro, anche in occasione di verifiche o ispezioni, in relazione all'osservanza degli obblighi previsti dalla normativa di riferimento in relazione: (**i**) alla predisposizione delle denunce relative alla costituzione, alla modifica e alla estinzione dei rapporti di lavoro; (**ii**) agli elenchi del personale attivo, assunto e cessato presso l'INAIL; (**iii**) a controllo e verifiche circa il rispetto

dei presupposti e delle condizioni previste dalla normativa vigente; e (**iv**) alla predisposizione ed esecuzione dei pagamenti verso lo Stato e gli altri enti pubblici

- Processi Sensibili principali: **I** e **VIII**

e) Gestione degli adempimenti e dei rapporti nei confronti dei funzionari pubblici in relazione al rispetto dei presupposti e delle condizioni richieste dalla normativa vigente per le assunzioni agevolate e per le assunzioni obbligatorie (*e.g.* piano formativo, durata, rispetto del limiti di età, ecc.), anche in occasione di verifiche, ispezioni e accertamenti, nonché nella gestione delle relative comunicazioni

- Processi Sensibili principali: **I** e **VIII**

f) Gestione degli adempimenti e dei rapporti nei confronti delle altre Autorità amministrative indipendenti in relazione allo svolgimento delle attività regolate dalla legge (*e.g.*, il Garante per la protezione dei dati personali), anche in occasione di verifiche, ispezioni e accertamenti, nonché nella gestione delle relative comunicazioni

- Processo Sensibile principale: **I**

g) Acquisto di beni, servizi e consulenze

- Processi Sensibili principali: **II** e **VII**

h) Selezione, assunzione e gestione del personale

- Processo Sensibile principale: **VIII**

i) Gestione degli omaggi, delle liberalità nonché delle spese di rappresentanza

- Processi Sensibili principali: **II** e **IX**

j) Gestione di sponsorizzazioni e donazioni

- Processi Sensibili principali: **II** e **IX**

k) Gestione dell'erogazione del credito

- Processo Sensibile principale: **VI**

l) Selezione dei Consulenti Finanziari abilitati all'offerta fuori sede

- Processo Sensibile principale: **III**

m) Gestione dei contenziosi

- Processo Sensibile principale: **X**

n) Trasmissione su supporti informatici a Pubbliche amministrazioni, Enti Pubblici o Autorità, per il tramite di Outsourcer esterni oppure tramite sistemi informativi interni

- Processi Sensibili principali: **I** e **XI**

1.4. Principi generali di comportamento

In relazione ai Reati nei rapporti con la Pubblica Amministrazione si intendono anzitutto integralmente richiamati anche ai fini del presente Modello sia il **Codice anticorruzione**, sia il **Codice Etico e di Comportamento** (con particolare riferimento agli artt. 13-17 dello stesso).

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché ai Consulenti abilitati all'offerta fuori sede.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate negli artt. 24 e 25 del Decreto e di violare i principi e le procedure aziendali richiamate nella presente Parte Speciale.

Più nello specifico, nell'ambito di tale divieto di carattere generale, è **proibito**:

- effettuare o promettere, di propria iniziativa o a seguito di sollecitazione, elargizioni di denaro – anche utilizzando risorse proprie e non della Banca (p.e., da conti privati) – o di altra utilità nei confronti di pubblici ufficiali, di incaricati di un pubblico servizio o di qualsiasi persona che vanti presunte o effettive conoscenze con gli stessi;
- offrire, accettare, promettere o autorizzare doni, omaggi (quali, p.e., inviti a eventi di intrattenimento o sportivi) od ogni altra gratuita prestazione al di fuori di quanto previsto dalla prassi e dalle procedure aziendali – *i.e.*, ogni forma di regalo offerto di non modico valore ed eccedente le normali pratiche commerciali o di cortesia o, comunque, rivolto – o interpretabile come potenzialmente rivolto – ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale; in particolare:
    - ai rappresentanti della Pubblica Amministrazione o a loro familiari non devono essere offerti, direttamente o indirettamente, regali, doni o gratuite prestazioni che possano apparire, comunque, connessi con il rapporto di affari con le società del Gruppo o del Gruppo Bancario o miranti a influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Banca;
    - anche in quei Paesi in cui offrire regali o doni costituisce una prassi diffusa in segno di cortesia, tali regali devono essere di natura appropriata e non contrastare con le disposizioni di legge né comunque poter essere interpretati come richiesta di favori in contropartita.
- accordare vantaggi di qualsiasi natura – quali, a titolo meramente esemplificativo e non esaustivo, promesse di assunzione, conferimento di incarichi di consulenza ecc. – in favore di rappresentanti della Pubblica Amministrazione italiana o straniera (o di loro parenti, amici o *partner* di affari) che possano determinare rivolti – o interpretabili come potenzialmente rivolti – ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale;
- effettuare pagamenti in denaro contante, fatto salvo per quanto si dirà *infra* in relazione alla c.d. *piccola cassa;*
- eseguire prestazioni o riconoscere compensi in favore dei Consulenti, dei Consulenti Finanziari e dei *Partner* che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari, in special modo al fine di conseguire erogazioni, contributi o finanziamenti agevolati;
- destinare eventuali somme ricevute da organismo pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti agevolati per scopi diversi da quelli cui erano destinati.

1.5. Principi specifici per le singole attività sensibili

Con precipuo riferimento alle Attività Sensibili individuate *supra* § 1.3, fermi i divieti generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Negoziazione, stipula ed esecuzione di contratti con enti pubblici di rilevanza nazionale e internazionale

i La Banca identifica il personale incaricato della gestione delle gare pubbliche con indicazione di compiti, ruoli e responsabilità;

- ✓ ***Control Owner*:** Responsabile della Direzione Commerciale – Direzione commerciale; Unità Organizzativa persone giuridiche e condizioni
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con la clientela istituzionale

ii La stipulazione di contratti o convenzioni con soggetti pubblici da parte della Banca a seguito della partecipazione o per il tramite di Consulenti finanziari abilitati all'offerta fuori sede o direttamente, a procedure a evidenza pubblica (quali, a titolo esemplificativo, aste pubbliche, appalti, concorsi, licitazioni

private, trattative private) deve essere condotta in conformità ai principi, criteri e disposizioni dettate dal presente Modello;

- ✓ ***Control Owner*:** Responsabile della Direzione Commerciale – Direzione commerciale; Unità Organizzativa persone giuridiche e condizioni
- ✓ ***Documentazione interna di riferimento:*** Procedura Gestione dei rapporti con la clientela istituzionale

iii La fase di decisione circa la partecipazione ad una gara pubblica, consistente soprattutto nelle valutazione delle condizioni tecniche e nella convenienza di redditività dell'operazione, nonché nella successiva determinazione della relativa quotazione economica, deve essere approvata dal Responsabile della Direzione commerciale, con la collaborazione delle direzioni tecniche competenti in relazione all'oggetto di gara (*e.g.*, gestioni finanziarie, prodotti strutturati ecc.) nel rispetto dei criteri, dei limiti e delle procedure dettati da Allianz Bank e dall'Amministratore Delegato;

- ✓ ***Control Owner*:** Responsabile della Direzione Commerciale – Direzione commerciale; Unità Organizzativa pianificazione e controllo
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con la clientela istituzionale

iv La Banca assicura che il processo di negoziazione, stipula ed esecuzione dei contratti con la clientela istituzionale sia tracciabile e preveda l'archiviazione dell'esito dei controlli effettuati nonché di tutta la documentazione inerente al rapporto con il cliente;

- ✓ ***Control Owner*:** Direzione Commerciale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con la clientela istituzionale

v La Banca deve dare debita evidenza alle operazioni di negoziazione, stipulazione, esecuzione di contratti e convenzioni con soggetti pubblici incaricati di un pubblico servizio mediante procedure negoziate o mediante procedure ad evidenza pubblica, essendo queste considerate, ai fini del presente Modello, come operazioni sensibili. A tal fine Allianz Bank ha individuato il Responsabile della Direzione Commerciale quale referente interno per le operazioni sensibili indicate. Il Referente interno deve: (**1**) all'inizio dell'operazione sensibile, ricevere dai segnalanti (Dipendenti o Consulenti abilitati all'offerta fuori sede) la «Scheda di evidenza», dalla quale deve risultare: (a) il nome del soggetto segnalante; (b) il nome dei responsabili gerarchici del soggetto segnalante; (c) il nominativo del soggetto appartenente alla Pubblica amministrazione e le caratteristiche del prodotto/servizio richiesto; (**2**) comunicare all'Organismo di Vigilanza l'avvio di una trattativa con un soggetto appartenente alla Pubblica Amministrazione; (**3**) predisporre e aggiornare nel corso dell'Operazione Sensibile, la scheda interna con i seguenti aspetti: (a) l'indicazione delle Direzioni/Unità Organizzative aziendali e dei relativi Dipendenti coinvolti, dell'eventuale controparte interessata, delle caratteristiche del prodotto/servizio da proporre alla Pubblica Amministrazione e del valore dell'Operazione Sensibile (comprensiva della quotazione economica); (b) gli elementi e circostanze attinenti l'Operazione Sensibile acquisiti nel corso della stessa (ad esempio, movimenti di denaro, nomina di eventuali consulenti, data in cui è stata presentata l'offerta, verifiche fatte su eventuali Partner, impegni e garanzie sottoscritte dal Partner); (c) cronologia delle attività poste in essere ai fini della realizzazione dell'Operazione Sensibile, incluse le riunioni svolte al riguardo con il soggetto appartenente alla Pubblica Amministrazione; (**4**) annotare e comunicare la necessaria preventiva approvazione per la realizzazione dell'Operazione Sensibile; (**5**) curare la documentazione delle eventuali riunioni con il soggetto appartenente alla Pubblica Amministrazione dalle quali scaturiscano decisioni rilevanti in merito all'Operazione Sensibile; (**6**) annotare la chiusura dell'Operazione Sensibile nella Scheda di evidenza ed inviare comunicazione all'Organismo di Vigilanza; (**7**) curare la manutenzione di un archivio delle Schede di evidenza e della eventuale documentazione a supporto da tenere a disposizione dell'Organismo di Vigilanza;

- ✓ ***Control Owner:*** Responsabile della Direzione Commerciale – Direzione commerciale; Unità Organizzativa persone giuridiche e condizioni

- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con la clientela istituzionale

b) Gestione degli adempimenti e dei rapporti con le Autorità di vigilanza; e

c) Gestione degli adempimenti e dei rapporti nei confronti dei funzionari della Guardia di Finanza, Agenzia delle Entrate, Camera di Commercio, Industria e Artigianato, Ufficio del Registro, Tribunale e altri enti competenti in materia fiscale, tributaria e societaria, nonché con le Autorità di pubblica sicurezza; e

d) Gestione degli adempimenti e dei rapporti nei confronti dei funzionari dell'Istituto Nazionale della Previdenza Sociale, dell'Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro, dell'Azienda Sanitaria Locale, dell'Ispettorato del Lavoro e della Direzione Provinciale del Lavoro; e

e) Gestione degli adempimenti e dei rapporti nei confronti dei funzionari pubblici in relazione al rispetto dei presupposti e delle condizioni richieste dalla normativa vigente per le assunzioni agevolate e per le assunzioni obbligatorie (*e.g.* piano formativo, durata, rispetto del limiti di età, ecc.); e

f) Gestione degli adempimenti e dei rapporti nei confronti delle altre Autorità amministrative indipendenti in relazione allo svolgimento delle attività regolate dalla legge

i Tutti i Dipendenti che intrattengono rapporti non ordinari con la Pubblica Amministrazione e con le Autorità di Vigilanza e di controllo, sono tenuti, oltre al rispetto di tutti i principi e le regole indicate nel presente Modello e nel Codice Etico e di Comportamento della Banca, a sottoscrivere una descrizione delle Operazioni Sensibili svolte;

ii Alle ispezioni giudiziarie, tributarie e amministrative (quali, p.e., relative al D.lgs. 81/ 2008, verifiche tributarie, verifiche dell'INPS, o delle Autorità di Vigilanza) devono partecipare i soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali, che verranno conservati dall'Organismo di Vigilanza;

iii Ciascun dipendente che intenda o abbia necessità di intrattenere rapporti istituzionali con la P.A. deve preventivamente rivolgersi alla struttura di volta in volta individuata dalle procedure aziendali al fine di impostare il contatto e il rapporto in maniera appropriata. Qualora non sia possibile informare preventivamente la struttura, il dipendente, che si trovi nelle condizioni di dover intrattenere rapporti istituzionali con la PA, informa la struttura deputata non appena concretamente possibile. Per particolari circostanze, che impediscano di informare preventivamente la struttura deputata, poiché discendenti da un obbligo di riservatezza in capo a Allianz Bank, la funzione aziendale preposta può decidere di autorizzare le differenti e più appropriate modalità di contatto e di svolgimento dei rapporti istituzionali con PA, fermo restando l'obbligo di informare la struttura a tal fine deputata, nel momento in cui tali obblighi di riservatezza siano venuti meno;

iv La Banca identifica il personale incaricato di intrattenere, nell'ambito delle proprie mansioni, rapporti con gli esponenti della Pubblica Amministrazione o di enti pubblici territoriali e non territoriali, con indicazione di compiti, ruoli, e responsabilità in accordo con le regole di segregazione dei compiti previste dalla Società e con il sistema di deleghe e procure adottato;

v La Banca identifica il personale incaricato alla gestione dei rapporti con la Pubblica Amministrazione nel caso di visite ispettive, con indicazione dei compiti, ruoli, e responsabilità in accordo con la stratificazione dei poteri delegati;

vi La Banca definisce e formalizza i compiti e comportamenti da adottare nel corso di eventuali visite ispettive e archivia i verbali predisposti a seguito delle stesse;

- ✓ ***Control Owner***: Unità organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con le Autorità di Vigilanza; Procedura Gestione richieste dalle Autorità giudiziarie e da Agenzia Entrate

g) Acquisti di beni, servizi e consulenze

i La Banca definisce e formalizza il *budget* annuale e il processo di approvazione delle spese *extra budget*;

- ✓ ***Control Owner**:* Unità organizzativa Pianificazione e controllo – Direzione commerciale
- ✓ ***Documentazione interna di riferimento***: Procedura Budgeting e pianificazione strategica; Procedura Gestione del ciclo passivo

ii La Banca, per le attività di *Procurement* gestite dalla funzione *Finance*, prevede livelli autorizzativi diversi a seconda dell'importo dell'acquisto e assicura che vi sia separazione di ruoli tra chi richiede l'acquisto e chi lo autorizza;

- ✓ ***Control Owner**:* Unità organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica; Procedura adempimenti in fase di definizione e sottoscrizione di contratti di acquisto di beni, servizi e prestazioni d'opera (DUVRI); Procedura Gestione del ciclo passivo; Regolamento sull'esercizio dei poteri delegati

iii Alle Società di Service, Consulenti e *Partner* che materialmente intrattengano rapporti con la Pubblica Amministrazione per conto della Banca, deve essere formalmente conferito potere in tal senso con apposita clausola contrattuale. Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta;

iv La Banca adotta una procedura aziendale per la gestione dei rapporti con Consulenti e Fornitori la quale prevede una verifica preliminare del possesso da parte degli stessi dei necessari requisiti di attendibilità e onorabilità dei fornitori aziendali prevedendo una lista di Consulenti e Fornitori "accreditati" e disciplina il processo di acquisto del bene/attività consulenziale, indicando le unità coinvolte;

- ✓ ***Control Owner**:* Unità Organizzativa Compliance e Antiriciclaggio; Unità Organizzativa Demand & Procurement Management
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo; Analisi Integrità del fornitore – Questionario di Autovalutazione del fornitore; Analisi Integrità del fornitore – Valutazione Allianz Bank; Procedura Vendor Integrity Screening (VIS) e Verifiche Aggiuntive (Carichi Pendenti)

v La Banca assicura la tracciabilità dell'intero processo di gestione degli acquisti;

- ✓ ***Control Owner**:* Unità Organizzativa Demand & Procurement Management
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo; Analisi Integrità del fornitore – Questionario di Autovalutazione del fornitore; Analisi Integrità del fornitore – Valutazione Allianz Bank; Procedura Vendor Integrity Screening (VIS) e Verifiche Aggiuntive (Carichi Pendenti)

vi I Fornitori e i Consulenti devono essere scelti con metodi trasparenti e secondo specifica procedura nel rispetto della quale la selezione deve avvenire tra i Fornitori e i Consulenti "accreditati" dalla Società; le richieste di spesa eventualmente rivolte a soggetti diversi devono essere accompagnate da adeguata motivazione e pur sempre nel rispetto della procedura aziendale;

- ✓ ***Control Owner***: Unità Organizzativa Demand & Procurement Management
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo; Procedura Vendor Integrity Screening (VIS) e Verifiche Aggiuntive (Carichi Pendenti)

vii La Banca attua una gara tra i fornitori accreditati in occasione di acquisti di beni e servizi per forniture superiori ad una soglia predeterminata ed indicata in apposita *policy* aziendale;

viii La Banca si è dotata di un'apposita procedura aziendale che regola la selezione dei Fornitori di beni e servizi esterni al Gruppo Allianz, con i quali venga sottoscritto uno o più contratti di fornitura che superino un importo di valore prestabilito;

- ✓ ***Control Owner**:* Unità Organizzativa Pianificazione e Controllo; Unità Organizzativa Demand & Procurement Management
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo; Procedura Vendor Integrity Screening (VIS) e Verifiche Aggiuntive (Carichi Pendenti)

ix La Banca effettua una valutazione periodica dei Fornitori di beni e sevizi con i quali venga sottoscritto uno o più contratti di fornitura che superino un importo di valore prestabilito al fine di monitorare l'operato degli stessi;

x La Banca monitora periodicamente il possesso dei requisiti di onorabilità e professionalità dei Fornitori ed eventualmente aggiorna le liste dei Fornitori "accreditati";

- ✓ ***Control Owner**:* Unità Organizzativa Demand & Procurement Management
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo; Procedura Vendor Integrity Screening (VIS) e Verifiche Aggiuntive (Carichi Pendenti)

xi I contratti tra Allianz Bank e le Società di Service, i Consulenti e i *Partner* devono essere definiti per iscritto in tutte le loro condizioni e termini e rispettare tutte le condizioni previste negli stessi;

- ✓ ***Control Owner**:* Unità Organizzativa Consulenza Legale Banca; Responsabile Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

xii Nei contratti con Consulenti, Fornitori e Appaltatori sarà inserita la specifica clausola *anti-corruption*, definita sulla base delle disposizioni impartite al Gruppo da Allianz SE;

xiii La Banca inserisce nei contratti con i Consulenti e Fornitori una specifica clausola con la quale gli stessi dichiarano: (i) di essere a conoscenza del D.lgs. 231/2001 e di non essere mai incorsi nella commissione di uno dei Reati; (ii) di prendere atto che la Banca ha adottato il presente Modello, pubblicato sul sito *web*; (iii) di impegnarsi al rispetto della normativa alla base del Modello e quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;

xiv Nei contratti con i Consulenti e i Fornitori deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.lgs. 231/2001 (es. clausole risolutive espresse);

- ✓ ***Control Owner**:* Unità Organizzativa Consulenza Legale Banca; Responsabile Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento:*** Procedura Gestione della contrattualistica

xv Prima di effettuare pagamenti relativi ad acquisti di beni/servizi la Società verifica l'avvenuta prestazione del servizio/ricezione del bene. Sono definite e formalizzate le attività di verifica dell'allineamento tra l'entrata merce/avvenuta prestazione del servizio, il relativo ordine d'acquisto e la fattura ricevuta dal Fornitore;

xvi La Banca definisce le spese gestibili tramite cassa contante indicando le modalità di rendicontazione da parte del soggetto che sostiene le spese e prevedendo attività di verifica della corretta rendicontazione;

xvii La Banca definisce ruoli e responsabilità per le attività di deposito e reintegro delle casse contanti;

- ✓ ***Control Owner**:* Unità Organizzativa Reti, Contabilità e Bilancio
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo

xviii La Banca prevede l'esecuzione e autorizzazione delle riconciliazioni della piccola cassa;

- ✓ ***Control Owner**:* Unità Organizzativa Reti, Contabilità e Bilancio; Responsabile dell'Unità organizzativa amministrazione; Responsabile dell'Unità Organizzativa Reti, Contabilità e Bilancio

- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo

h) Selezione, assunzione e gestione del personale

i La Banca adotta una *policy* che prevede la redazione annuale di un piano di fabbisogno di risorse umane a livello aziendale e condivide il medesimo a livello collegiale;

- ✓ ***Control Owner****:* Unità Organizzativa Risorse Umane (per la predisposizione del Piano Risorse); Responsabile della Direzione Risorse (per le strategie definite nell'ambito del processo di Strategic Dialogue e del budget)
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e valutazione del personale e politiche retributive

ii La Banca adotta una procedura che disciplina l'interazione tra i diversi uffici coinvolti nella selezione e assunzione del personale;

iii La Banca adotta una *policy* che prevede la tracciabilità di ogni fase e la collegialità del processo decisionale di assunzione del personale (anche dirigente);

- ✓ ***Control Owner****:* Unità Organizzativa Risorse Umane; Responsabile della Direzione Risorse
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e valutazione del personale e politiche retributive

iv La selezione e assunzione del personale è ispirata a un criterio di trasparenza sulla base dei seguenti parametri: (a) professionalità adeguata rispetto all'incarico o alle mansioni da assegnare; (b) uguaglianza di trattamento tra i diversi candidati; (c) affidabilità rispetto al rischio di infiltrazione criminale. Per tale ragione, la Banca assicura che vengano prodotti prima della consegna della lettera d'assunzione i seguenti documenti: il *curriculum vitae*; il certificato generale del casellario giudiziale completo delle disposizioni della banca dati del casellario Europeo, la dichiarazione relativa ad eventuali rapporti di lavoro presso la Pubblica Amministrazione. È cura della Banca conservare la documentazione esibita in sede di assunzione, anche al fine di consentine la consultazione da parte dell'Organismo di Vigilanza nell'espletamento della sua funzione di vigilanza sul rispetto del Modello;

- ✓ ***Control Owner****:* Unità Organizzativa Risorse umane
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e valutazione del personale e politiche retributive; Procedura Gestione degli adempimenti amministrativi

v La Banca ha adottato una specifica procedura che prevede una predeterminazione della tipologia di spese rimborsabili; il rimborso delle spese, in particolare, può essere effettuato solo a seguito della presentazione di idonei giustificativi;

- ✓ ***Control Owner****:* Unità Organizzativa Risorse umane
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione degli adempimenti amministrativi

vi La Banca prevede l'approvazione del rimborso da parte di funzione diversa rispetto a quella cui appartiene la persona che richiede il rimborso;

- ✓ ***Control Owner****:* Responsabile della Direzione/Unità Organizzativa per l'autorizzazione della richiesta di rimborso spese; Unità Organizzativa Risorse Umane per l'elaborazione della richiesta di rimborso spese
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione degli adempimenti amministrativi

vii La Banca definisce le modalità di assegnazione e utilizzo delle carte di credito aziendali e le modalità di rendicontazione da parte del titolare delle carte.

i) Gestione degli omaggi, delle liberalità e delle spese di rappresentanza

i La Banca si è dotata di una *policy* interna in tema di omaggi che regola omaggi e regalie. È necessario in ogni caso chiedere l'approvazione da parte del Responsabile di Direzione/Unità Organizzativa, previa consultazione altresì dell'Unità organizzativa Compliance e Antiriciclaggio di Allianz Bank al fine di offrire, promettere o autorizzare qualsivoglia forma di regalo o omaggio in favore di un funzionario pubblico;

ii La Banca adotta una *policy* che prevede la possibilità di effettuare regali e inviti a patto che: (i) rientrino nelle consuete pratiche commerciali; (ii) non siano esageratamente generosi, eccessivi o sconvenienti; (iii) non possano essere interpretati come una forma di persuasione inappropriata; (iv) non influenzino impropriamente il giudizio del destinatario; (v) non violino *policy* e procedure adottate dalla Banca e dal Gruppo (tra cui il Codice Anticorruzione);

- ✓ ***Control Owner**:* Unità organizzativa Compliance e antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Erogazioni liberali; Codice di condotta in materia di regali e intrattenimento; Codice Etico e di comportamento; Codice Anticorruzione Gruppo Bancario Allianz Bank

iii I regali e gli omaggi, offerti o ricevuti, devono essere documentati in modo adeguato e trasparente, in conformità a quanto espressamente previsto dalla procedura di registrazione e approvazione fissata dall'Ordine di servizio in materia di regali e intrattenimento; in caso di dubbio, occorre darne tempestiva informazione alla Funzione *Compliance* di Allianz S.p.A. ai fini di una opportuna valutazione;

- ✓ ***Control Owner**:* Unità organizzativa Compliance e antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Codice di condotta in materia di regali e intrattenimento

iv La Banca adotta una *policy* che prevede una valutazione collegiale preventiva adeguatamente motivata e documentata in relazione a regali ed inviti che possano potenzialmente presentare criticità ai fini della normativa in esame (sulla base di parametri fissati con apposita *policy* aziendale) e conseguente autorizzazione all'effettuazione dei medesimi solo laddove, a seguito dell'analisi effettuata, vengano ritenute di fatto insussistenti le suddette criticità;

- ✓ ***Control Owner***: Unità organizzativa Compliance e antiriciclaggio
- ✓ ***Documentazione di riferimento***: Procedura Erogazioni liberali; Codice di condotta in materia di regali e intrattenimento; Codice Anticorruzione Gruppo Bancario Allianz Bank

v La Banca adotta specifica *policy* che prevede una predeterminazione della tipologia di spese rimborsabili; il rimborso delle spese, in particolare, può essere effettuato solo a seguito della presentazione di idonei giustificativi;

- ✓ ***Control Owner**:* Direzione Risorse
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle spese di ospitalità e di rappresentanza; Procedura Gestione degli adempimenti amministrativi

vi La Banca adotta una *policy* che prevede che l'approvazione del rimborso avvenga da parte di funzione diversa rispetto a quella cui appartiene la persona che richiede il rimborso;

- ✓ ***Control Owner**:* Responsabile della Direzione/Unità Organizzativa per l'autorizzazione della richiesta di rimborso spese; Direzione Risorse per l'elaborazione della richiesta di rimborso spese
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle spese di ospitalità e di rappresentanza; Procedura Gestione degli adempimenti amministrativi

j) Gestione delle sponsorizzazioni e delle donazioni

i La Banca si è dotata di un sistema di *governance* delle donazioni;

- ✓ ***Control Owner**:* Unità Organizzativa Compliance e antiriciclaggio

- ✓ ***Documentazione interna di riferimento***: Procedura Erogazioni liberali; Procedura Gestione delle sponsorizzazioni della Banca

ii La Società effettua una verifica preventiva circa l'onorabilità dei destinatari della sponsorizzazione e prevede la tracciatura e la collegialità del processo autorizzativo di concessione della contribuzione;

- ✓ ***Control Owner****:* Unità Organizzativa Controlli Banca
- ✓ ***Documentazione interna di riferimento***: Procedura Erogazioni liberali; Procedura Gestione delle sponsorizzazioni della Banca

iii La Banca definisce un *budget* per le sponsorizzazioni e prevede modalità e livelli autorizzativi per l'approvazione di spese *extra-budget*;

iv La Società prevede che le richieste di sponsorizzazione aventi ad oggetto un contributo annuo superiore a Euro 50.000 preliminarmente alla stipula del relativo contratto, devono essere sottoposte dal Responsabile della Direzione Risorse, per la relativa approvazione, al GMM (Group Marketing Management) Sponsoring Team della Capogruppo Allianz SE. Inoltre, qualunque richiesta di sponsorizzazione deve essere sottoposta all'Amministratore Delegato previa autorizzazione da parte dell'Unità Organizzativa Controlli Banca;

- ✓ ***Control Owner****:* Responsabile della Direzione Risorse; Unità Organizzativa Pianificazione e Controllo
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle sponsorizzazioni della Banca; Procedura Manuale Antiriciclaggio; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma

k) Gestione dell'erogazione del credito

i La Banca prevede che qualunque erogazione dei fondi debba essere deliberata previa adeguata istruttoria alla quale partecipano soggetti e funzioni diverse all'interno della Banca, in modo da minimizzare il rischio di una manipolazione illecita dei dati ed aumentare la condivisione delle conoscenze e delle decisioni all'interno della Banca;

ii Qualunque erogazione dei fondi deve presupporre una approfondita conoscenza della clientela, così da consentire una valutazione della coerenza e della compatibilità dell'operazione con il profilo cliente, soprattutto laddove quest'ultimo non svolga attività di rilievo economico;

- ✓ ***Control Owner****:* Unità Organizzativa Crediti; Unità Organizzativa Monitoraggio e Crediti Anomali: Unità Organizzativa Concessioni Nord/Concessioni Sud; Unità Organizzativa Crediti Corporate; Unità Organizzativa Private Credit Specialist; Unità Organizzativa Controlli Rete e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Perfezionamento contrattuale ed erogazione; Procedura Monitoraggio del credito; Procedura Concessione affidamenti a clienti privati e imprese; Regolamento per la gestione del credito

iii L'erogazione del credito da parte di Allianz Bank deve essere eseguita nel rispetto delle regole aziendali previste nel Regolamento per la gestione del credito, predisposto in ottemperanza alle norme di riferimento che regolano gli affidamenti (e in particolare a quelle del Testo Unico Bancario) e alle istruzioni di vigilanza per le Banche;

- ✓ ***Control Owner****:* Unità Organizzativa crediti
- ✓ ***Documentazione interna di riferimento***: Procedura Perfezionamento contrattuale ed erogazione; Procedura Monitoraggio del credito; Procedura Concessione affidamenti a clienti privati e imprese; Regolamento per la gestione del credito

l) Selezione dei Consulenti Finanziari abilitati all'offerta fuori sede

i La Banca prevede che i Consulenti Finanziari debbano essere selezionati con metodi trasparenti e secondo specifica procedura di selezione condotta nel rispetto di criteri di professionalità, integrità e imparzialità;

- ✓ ***Control Owner**:* Direzione Commerciale
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e reclutamento dei Consulenti Finanziari abilitati all'offerta fuori Sede Diretti (PFD) e dei Produttori assicurativi (PA); Procedura Selezione e reclutamento dei Consulenti finanziari abilitati all'offerta fuori Sede (di Agenzia)

ii La Banca verifica l'attendibilità e l'onorabilità degli intermediari che collocano prodotti bancari e finanziari per conto della stessa prima dell'instaurazione del rapporto e, periodicamente, anche in costanza di rapporto;

- ✓ ***Control Owner**:* Unità Organizzativa Sviluppo Commerciale Nord o Centro-Sud
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e reclutamento dei Consulenti Finanziari abilitati all'offerta fuori Sede Diretti (PFD) e dei Produttori assicurativi (PA); Procedura Selezione e reclutamento dei Consulenti finanziari abilitati all'offerta fuori Sede (di Agenzia)

iii. La Banca affida la distribuzione dei propri prodotti a soggetti autorizzati dall'Autorità di Vigilanza;

- ✓ ***Control Owner**:* Struttura Manageriale di Rete (Area Manager, Executive Manager e Business Manager); Unità Organizzativa Rete PFA (per il reclutamento dei Consulenti Finanziari abilitati all'offerta fuori Sede di Agenzia (PFA)); Unità Organizzativa Rete FA (per il reclutamento dei Consulenti Finanziari abilitati all'offerta fuori Sede Diretti (PFD) e dei Produttori assicurativi (PA))
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e reclutamento dei Consulenti Finanziari abilitati all'offerta fuori Sede Diretti (PFD) e dei Produttori assicurativi (PA); Procedura Selezione e reclutamento dei Consulenti finanziari abilitati all'offerta fuori Sede (di Agenzia)

iv. La Banca monitora periodicamente il possesso dei requisiti dell'affidabilità e onorabilità in capo ai Consulenti Finanziari abilitati all'offerta fuori sede;

v. La Banca prevede condizioni contrattuali standardizzate relative ai prodotti collocati, non modificabili in senso peggiorativo per il cliente finale;

- ✓ ***Control Owner**:* Unità organizzativa legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

iii. La Banca adotta un modello di remunerazione dei Consulenti Finanziari abilitati all'offerta fuori sede e delle figure interne alla Banca responsabili delle aree di *business* in esame, tale da disincentivare condotte corruttive;

- ✓ ***Control Owner**:* Responsabile della Direzione Risorse (per le strategie definite nell'ambito del processo di Strategic Dialogue e del budget)
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle incentivazioni ai Consulenti finanziari abilitati all'offerta fuori sede

iv. La Banca effettua costanti controlli *ex post* sulla rete dei Consulenti Finanziari abilitati all'offerta fuori sede al fine di verificare l'eventuale collocamento di prodotti non nell'interesse del cliente finale;

- ✓ ***Control Owner**:* Unità Organizzativa Analisti Rete; Unità Organizzativa Ispettori Rete
- ✓ ***Documentazione interna di riferimento***: Procedura Controlli sulla Rete dei Consulenti finanziari abilitati all'offerta fuori Sede

v. La Banca effettua attività di sensibilizzazione e formazione (verificando adesione e apprendimento) nei confronti del personale e dei Consulenti Finanziari abilitati all'offerta fuori sede sulla tematica della corruzione;

- ✓ ***Control Owner**:* Unità Organizzativa Sviluppo Professionale Risorse
- ✓ ***Documentazione interna di riferimento***: Procedura Formazione dei Consulenti finanziari abilitati all'offerta fuori Sede

vi. La Banca inserisce nei contratti con Consulenti, Fornitori e *Partner* una specifica clausola con la quale gli stessi dichiarano: (i) di essere a conoscenza del D.lgs. 231/2001 e di non essere mai incorsi nella commissione di uno dei reati in discorso; (ii) di prendere atto che la Banca ha adottato il presente Modello, pubblicato sul sito *web*; (iii) di impegnarsi al rispetto della normativa alla base del Modello e quindi a non porre in essere comportamenti tali da configurare una delle ipotesi di Reato dal medesimo previste;

vii. Negli accordi con i Consulenti Finanziari abilitati all'offerta fuori sede deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.lgs. 231/2001 (es. clausole risolutive espresse) ed altresì la specifica clausola *anti-corruption*;

- ✓ ***Control Owner**:* Unità Organizzativa Consulenza Legale Banca; Responsabile Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

m) Gestione dei contenziosi

i La Banca definisce ruoli e responsabilità dei soggetti incaricati di gestire il singolo contenzioso o posizioni in pre-contenziosa;

- ✓ ***Control Owner**:* Unità Organizzativa Consulenza Legale Rete
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del contenzioso

ii Per la gestione di contenziosi, ai legali esterni deve essere richiesta specifica dichiarazione di rispetto da parte degli stessi delle norme di cui al D.lgs. n. 231/2001 e dei principi in tale ambito adottati dalla Banca;

- ✓ ***Control Owner**:* Unità organizzativa consulenza legale Banca
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

iii La Banca prevede che l'eventuale coinvolgimento di consulenti legali esterni avvenga solo previa verifica dell'attendibilità e dell'onorabilità dei medesimi;

- ✓ ***Control Owner**:* Unità Organizzativa Compliance e Antiriciclaggio; Unità Organizzativa Consulenza Legale Banca
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del ciclo passivo

iv La Banca prevede la partecipazione di più soggetti al processo decisionale e la tracciabilità delle singole fasi di apertura e gestione del contenzioso e dei relativi accordi transattivi;

v La Società prevede che il processo che conduce ad un accordo transattivo sia adeguatamente tracciato e che gli eventuali accordi transattivi siano debitamente formalizzati, sottoscritti in coerenza con il sistema autorizzativo in essere e correttamente archiviati;

- ✓ ***Owner**:* Responsabile dell'Unità Organizzativa Legale; Unità Organizzativa Consulenza Legale Rete
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del contenzioso

vi. Nel caso in cui non sia possibile optare per un nominativo già censito all'interno dell'apposito elenco dei legali esterni accreditati, la Banca si avvale di studi legali esterni per l'assistenza nella causa/procedimento instaurato, la cui selezione è condotta dall'Unità Organizzativa Legale di Allianz Bank;

- ✓ ***Control Owner**:* Unità Organizzativa Consulenza Legale Rete (per la valutazione delle candidature di legali esterni non presenti nella Recommended List); Responsabile dell'Unità Organizzativa Legale (per la selezione del legale esterno)

- ✓ ***Documentazione interna di riferimento***: Procedura Gestione del contenzioso

n) Trasmissione di dati su supporti informatici a Pubbliche Amministrazioni, Enti pubblici o Autorità, per il tramite di *outsourcer* esterni oppure tramite sistemi informativi esterni

i Nei confronti della Pubblica Amministrazione, Allianz Bank svolge l'attività di generazione periodica di flussi informativi verso soggetti della Pubblica Amministrazione, per il tramite di *outsourcer* esterni -*e.g.*, Consorzio fra istituti bancari - oppure tramite sistemi informativi interni il cui utilizzo è limitato a personale autorizzato e prevede procedure di verifica di liceità e correttezza dei dati trasmessi. In aggiunta è fatto divieto al personale di installare o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (es. sistemi per individuare le password, decifrare i file criptati, sfruttare vulnerabilità) sia di sistemi interni che esterni;

- ✓ ***Control Owner****:* Unità Organizzativa Compliance e Antiriciclaggio; Unità Organizzativa Segreteria Societaria
- ✓ ***Documentazione interna di riferimento***: Procedura Comunicazioni alle Autorità di Vigilanza e ad altri Enti esterni

ii Le Società di Service per la fornitura dei servizi di natura informatica sono tenute a gestire il servizio informatico nel rispetto di tutte le regole e principi previsti nel Modello, garantendo l'esatto adempimento a favore di Allianz Bank di tutte le procedure e i controlli informatici tipici di un sistema informativo integrato, volti a garantire l'integrità e la sicurezza dei dati;

- ✓ ***Control Owner****:* Unità Organizzativa Organizzazione e Sviluppo Applicativo
- ✓ ***Documentazione interna di riferimento***: Procedura Controlli sull'operatività degli outsourcer informatici; Policy di esternalizzazione di funzioni aziendali

iii Amos Italia e le società di service per la fornitura dei servizi di natura informatica sono tenute a gestire il servizio informatico nel rispetto di tutte le regole e principi previsti nel Modello, garantendo l'esatto adempimento a favore di Allianz Bank di tutte le procedure e i controlli informatici tipici di un sistema informativo integrato, volti a garantire l'integrità e la sicurezza dei dati;

- ✓ ***Control Owner****:* Unità Organizzativa Organizzazione e Sviluppo Applicativo
- ✓ ***Documentazione interna di riferimento***: Procedura Controlli sull'operatività degli outsourcer informatici; Policy di esternalizzazione di funzioni aziendali

2. Reati informatici e trattamento illecito di dati

2.1. Le fattispecie di reato rilevanti di cui all'art. 24-*bis*, D.lgs. 231/2001

FALSITÀ DI UN DOCUMENTO INFORMATICO PUBBLICO AVENTE EFFICACIA PROBATORIA (ART. 491-*BIS* C.P.)

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

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti cartacei: per *documento informatico*, in particolare, deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Esempi

Un Dipendente della Banca inserisce fraudolentemente dei dati falsi in banche dati pubbliche.

Un Dipendente della Banca deliberatamente modifica gli archivi informatici della Società in modo da falsificare i dati o i documenti ivi contenuti.

Un Dipendente della Banca utilizza in maniera fraudolenta il dispositivo di firma digitale per inviare documenti aventi valore legale o probatorio come, p.e., il bilancio civilistico della Società o la modulistica F24.

Un Dipendente della Banca cancella o altera le informazioni a valenza probatoria salvate sui sistemi informatici della Società, allo scopo di eliminare le prove di un reato.

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

Il reato di cui all'art. 615-*ter* c.p. punisce chiunque 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.

Questo illecito penale rientra tra i delitti contro la libertà individuale: il bene che viene protetto dalla norma, secondo l'interpretazione prevalente, è il c.d. «*domicilio informatico*», benché vi sia un orientamento che ravvisa come bene tutelato l'integrità dei dati e dei programmi contenuti nel sistema informatico.

La norma prevede due condotte distinte, l'*accesso* a un sistema e il *mantenimento* nel sistema: l'accesso deve essere abusivo e deve riguardare un sistema protetto da una misura di sicurezza (*i.e.*, anche da una semplice *password*); viceversa, il mantenimento nel sistema integra la fattispecie quando è effettuato contro la volontà del titolare del sistema.

Secondo l'interpretazione della giurisprudenza, il reato sussiste quando la condotta di accesso o mantenimento nel sistema posta in essere dall'agente, benché abilitato all'accesso, violi le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema o quando l'agente ponga in essere operazioni di natura diversa da quelle per le quali l'accesso gli è consentito. Non rilevano, quindi, i motivi che hanno indotto all'ingresso nel sistema, mentre è rilevante la violazione delle prescrizioni di carattere organizzativo circa le modalità di accesso agli strumenti informatici (*i.e.* disposizioni organizzative interne, prassi aziendali, clausole di contratti individuali di lavoro, ecc.).

Si noti che, secondo il più recente indirizzo giurisprudenziale, il reato in esame può *concorrere* con la frode informatica *ex* art. 640-*ter* c.p. analizzata in precedenza mentre, in considerazione della sua maggiore gravità a fronte della tutela del medesimo bene giuridico, *assorbe* il reato punito dall'art. 615-*quater* c.p. esaminato *infra*.

Esempio

Un Dipendente della Banca si introduce nel sistema informatico di un'altra banca protetto da password di accesso così da carpire dati riservati.

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

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

Rilevano, dunque, condotte *preliminari* all'accesso abusivo, poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico. I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, *password* o schede informatiche.

Esempio

Un Dipendente della Banca si procura abusivamente i codici di accesso al sistema informatico di un'altra banca per accedere a informazioni sulle caratteristiche di prodotti finanziari commercializzata dalla stessa.

DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-*QUINQUIES* C.P.)

L'art. 615-*quinquies* c.p. punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Questo delitto è integrato, ad esempio, nel caso in cui il soggetto si procuri un *virus*, idoneo a danneggiare un sistema informatico o qualora si producano o si utilizzino delle *smart card* che consentono il danneggiamento di apparecchiature o di dispositivi elettronici. È necessaria la sussistenza dello scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, di favorire l'interruzione parziale o totale o l'alterazione del suo funzionamento.

Esempio

Un Dipendente della Banca invia a un lavoratore di una banca concorrente un programma infettato da un virus, allo scopo di danneggiarne il sistema informatico.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-*QUATER* C.P.)

L'art. 617-*quater* c.p. punisce, a querela della persona offesa, chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, oppure, ancora, rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni medesime. Il secondo comma della medesima disposizione, viceversa, rende procedibile d'ufficio – e innalza la pena della reclusione - se il fatto è commesso: (**i**) in danno di un sistema informatico o telematico utilizzato dallo Stato, da un altro ente pubblico o da un'impresa esercente servizi pubblici o di pubblica necessità; (**ii**) da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; (**iii**) da chi esercita anche abusivamente la professione di investigatore privato.

Secondo l'interpretazione maggioritaria del reato in esame, la fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione. Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale, ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in

cui la comunicazione sia rivolta a un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Nell'ipotesi del secondo comma, invece, non è necessario che le comunicazioni siano state intercettate in modo fraudolento, in quanto la norma persegue il fine di evitare che siano divulgate con qualsiasi mezzo di informazione al pubblico comunicazioni c.d. *chiuse*, ossia destinate a rimanere segrete.

Esempio

Un Dipendente della Banca esegue attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazione di una banca concorrente.

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-*QUINQUIES* C.P.)

Questo reato punisce chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

La condotta vietata dall'art. 617-*quinquies* c.p. è quindi costituita della mera installazione di apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate. Si tratta di un reato che mira a prevenire condotte di intercettazione, impedimento o interruzione di comunicazione informatiche o telematiche.

Esempio

Un Dipendente della Banca installa apparecchiature allo scopo di intercettare le comunicazioni email di uno o più dipendenti di una banca concorrente.

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

Tale reato si configura quando un soggetto distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui. Secondo la costante interpretazione giurisprudenziale, in particolare, per *dato* si intende la rappresentazione di informazioni o concetti che, essendo destinate alla elaborazione da parte di un *computer*, sono codificate in forma elettronica, magnetica, ottica o, comunque, non percettibile visivamente; per *programma informatico*, invece, si intende un insieme di dati; per *informazione*, infine, si intende quelle incorporate su un supporto materiale.

Esempio

Un Dipendente della Banca procede alla cancellazione di dati dalla memoria di un computer aziendale senza essere stato preventivamente autorizzato da parte delle competenti funzioni della Società.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITÀ (ART. 635-*TER* C.P.)

Questo reato si realizza quando un soggetto commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altri ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha a oggetto beni dello Stato, di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il reato sussiste anche nel caso in cui si tratti di dati, informazioni o programmi informatici di proprietà di privati ma destinati alla soddisfazione di un interesse pubblico.

Perché il reato venga integrato è sufficiente che si tenga una condotta finalizzata alla distruzione, deterioramento, cancellazione, alterazione o soppressione dei dati, delle informazioni e dei programmi informatici.

Esempio

Un Dipendente della Banca, riuscendo ad accadervi da remoto, procede alla cancellazione dei dati della memoria di un computer di un funzionario di una autorità di vigilanza a seguito di una ispezione avviata nei confronti della Società.

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

Tale reato si realizza quando un soggetto, mediante le condotte dell'art. 635-*bis* c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

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

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

Esempio

Un Dipendente della Banca esegue attività di sabotaggio industriale trasmettendo un virus ai domini e-mail di una banca concorrente al fine di intasare e rendere inservibile il sistema informatico della stessa nel corso di una procedura di gara online.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635-*QUINQUIES* C.P.)

Questo reato si configura quando il «*fatto di cui all'art. 635*-quater» è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibile sistemi informatici o telematici di pubblica utilità o a ostacolarne gravemente il funzionamento.

In questo caso, quindi, i sistemi oggetto dell'attività aggressiva possono essere esclusivamente quelli di *pubblica utilità*, cioè messi al servizio di una collettività indifferenziata di persone; gli stessi possono appartenere tanto a privati quanto a enti pubblici.

Esempio

Un Dipendente della Banca, riuscendo ad accedervi da remoto, danneggia il sistema di video sorveglianza di un ente pubblico.

2.2. Processi e attività sensibili rilevanti

In relazione ai delitti informatici e al trattamento illecito di dati sino a qui descritti, il Processo Sensibile della Banca potenzialmente più esposto al rischio di commissione di illeciti è il seguente:

XI. Utilizzo dei sistemi informatici aziendali

Nello specifico, all'interno del Processo Sensibile, sono state individuate le seguenti Attività Sensibili:

a) Utilizzo da parte del personale della rete aziendale, nonché accesso e modifica dei dati contenuti nelle banche dati elettroniche, nei sistemi gestionali e di produzione da parte di soggetti con profilo di "*System Administrator*" e/o profilo di *superuser*

- Processo Sensibile principale: **IX**

b) Gestione, manutenzione e sviluppo della rete aziendale

- Processo Sensibile principale: **IX**

2.3. Principi generali di comportamento

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, i Consulenti Finanziari abilitati all'offerta fuori sede, i Dirigenti e i membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali, a tutti i soggetti che operano in Allianz Technology S.p.A, società del Gruppo che fornisce alla Società le attività di erogazione, gestione e sviluppo dei servizi IT.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 24-*bis* del Decreto e di violare i principi e le procedure aziendali richiamate nella presente Parte Speciale.

Più nello specifico, nell'ambito di tale divieto di carattere generale, è **proibito**:

- divulgare informazioni relative ai sistemi informatici aziendali;
- utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta;
- modificare in qualsiasi modo la configurazione delle postazioni di lavoro fisse o mobili assegnate dalla Banca;
- installare o comunque utilizzare strumenti *software* o *hardware* che potrebbero essere adoperati per analizzare o compromettere la sicurezza di sistemi informatici o telematici (come, p.e., sistemi per individuare *password*, decifrare *file* criptati, ecc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, o di terzi con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Banca;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale di clienti o di terzi, comprensivo di dati, archivi e programmi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali;
- divulgare, cedere o condividere con personale interno o esterno alla Banca le proprie credenziali di accesso ai sistemi ed alla rete aziendale o di terzi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terzi per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- violare i sistemi informatici di società concorrenti per acquisire la loro documentazione;
- danneggiare le infrastrutture tecnologiche di società concorrenti al fine di impedirne l'attività o danneggiarne l'immagine;
- manipolare i dati presenti sui propri sistemi come risultato dei processi di *business*;
- danneggiare, distruggere o manomettere documenti informatici aventi efficacia probatoria, registrati presso enti pubblici (es. polizia, uffici giudiziari, ecc.), e relativi a procedimenti o indagini giudiziarie in cui la Banca sia coinvolta a qualunque titolo.

2.4. Principi specifici per le singole attività sensibili

Con precipuo riferimento alle Attività Sensibili individuate supra § 2.2, fermi i divieti generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Utilizzo da parte del personale della rete aziendale; e

b) Gestione, manutenzione e sviluppo della rete aziendale.

i La Banca, al fine di limitare le rischiosità connesse alle tipologie di reato qui considerate fornisce ai Destinatari un'adeguata informazione circa il corretto utilizzo degli *username* e delle *password* per accedere ai principali sistemi informatici utilizzati presso la Società e, in particolare, informa adeguatamente i Destinatari dell'importanza di mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi, della necessità di non lasciare incustoditi i propri sistemi informatici, della necessità di spegnere i propri sistemi informatici al termine della giornata lavorativa;

ii La Banca imposta i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;

iii La Banca fornisce un accesso da e verso l'esterno (connessione alla rete Internet) esclusivamente ai sistemi informatici dei Destinatari che ne abbiano necessità ai fini lavorativi;

- ✓ ***Control Owner****:* Unità Organizzativa Information Security Office
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Gestione e controllo degli accessi; Procedura Gestione degli incidenti di sicurezza informatica

iv La Banca predispone e mantiene adeguate difese fisiche a protezione dei *server* della Società;

v La Banca protegge per quanto possibile ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative a un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

- ✓ ***Control Owner****:* Allianz Technology S.p.A.
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Gestione e controllo degli accessi; Procedura Gestione degli incidenti di sicurezza informatica

vi La Banca si assicura che tutte le connessioni a reti aziendali da reti esterne devono avvenire tramite *firewall* e che le reti private virtuali sono configurate e gestite dagli *outsourcer* IT in accordo con le richieste e le indicazioni fornite;

- ✓ ***Control Owner****:* Allianz Technology S.p.A.
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Controlli sull'operatività degli outsourcer informatici; Procedura Gestione e controllo degli accessi; Procedura Gestione degli incidenti di sicurezza informatica; Procedura Gestione dei cambiamenti; Procedura Gestione delle applicazioni sviluppate dalle unità operative e di controllo

vii La Banca mantiene una documentazione, aggiornata nel tempo, di tutte le connessioni ad altre reti, le tipologie di rete, le componenti di rete e la configurazione di questi componenti;

- ✓ ***Control Owner****:* Unità Organizzativa Information Security Office
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Controlli sull'operatività degli outsourcer informatici; Procedura Gestione e controllo degli accessi; Procedura Gestione degli incidenti di sicurezza informatica; Procedura Gestione dei cambiamenti; Procedura Gestione delle applicazioni sviluppate dalle unità operative e di controllo

viii La Banca si assicura che l'accesso ai dati ed alle applicazioni aziendali sia limitato al solo il personale autorizzato. Tali permessi sono assegnati in accordo ad una procedura formalizzata e sono verificati periodicamente tramite sistemi automatici e con il coinvolgimento dei responsabili degli utenti;

- ✓ ***Control Owner****: :* Unità Organizzativa Information Security Office; Unità Organizzativa Organizzazione e Sviluppo Applicativo
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Controlli sull'operatività degli outsourcer informatici; Procedura Gestione e controllo degli accessi; Procedura Gestione

degli incidenti di sicurezza informatica; Procedura Gestione dei cambiamenti; Procedura Gestione delle applicazioni sviluppate dalle unità operative e di controllo

ix La Banca ha definito delle regole di assegnazione e composizione delle credenziali necessarie per l'accesso ai sistemi informativi aziendali;

- ✓ ***Control Owner**: :* Unità Organizzativa Information Security Office; Unità Organizzativa Organizzazione e Sviluppo Applicativo; Direzione/Unità Organizzativa interessata
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Controlli sull'operatività degli outsourcer informatici; Procedura Gestione e controllo degli accessi; Procedura Gestione delle patch di sicurezza; Procedura Gestione degli incidenti di sicurezza informatica; Procedura Gestione dei cambiamenti; Procedura Gestione delle applicazioni sviluppate dalle unità operative e di controllo; Procedura Gestione delle frodi informatiche relative ai pagamenti via internet

x Al fine di poter gestire al meglio la sicurezza delle informazioni, la Banca ha istituito un'unità organizzativa ad hoc (*Information Security Office*) che si occupa di: (i) gestire gli incidenti di sicurezza informatica, con l'obiettivo di identificare tempestivamente e minimizzare l'impatto di eventi avversi in ambito di sicurezza informatica, garantendo il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolte; (ii) gestire le frodi informatiche, sia potenziali sia reali, effettuate a danno dei clienti della Banca, al fine di ottenere accesso indebito ai canali messi a disposizione dalla medesima per effettuare pagamenti via internet; (iii) gestire e controllare gli accessi alle applicazioni del sistema informativo aziendale;

- ✓ ***Control Owner**: :* Unità Organizzativa Information Security Office
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Controlli sull'operatività degli outsourcer informatici; Procedura Gestione e controllo degli accessi; Procedura Gestione delle patch di sicurezza; Procedura Gestione degli incidenti di sicurezza informatica; Procedura Gestione dei cambiamenti; Procedura Gestione delle applicazioni sviluppate dalle unità operative e di controllo; Procedura Gestione delle frodi informatiche relative ai pagamenti via internet

xi La Banca fornisce ogni sistema informatico di adeguati *firewall* e *antivirus* e fa sì che, ove possibile, questi non possano venir disattivati;

xii La Banca limita l'accesso alle aree e ai siti particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. *virus*) capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti;

xiii Qualora per la connessione alla rete *internet* si utilizzino collegamenti *wireless*, la Banca protegge gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Banca, possano illecitamente collegarsi alla rete tramite i *router* della stessa e compiere illeciti ascrivibili ai Dipendenti;

xiv La Banca limita l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei destinatari (ad esempio, oltre allo *username* ed alla *password*, fornire ai soggetti che abbiano necessita di collegarsi alla rete societaria dall'esterno un "*token*" - una chiavetta - in grado di generare *password* casuali necessarie per l'accesso).

- ✓ ***Control Owner**:* Allianz Technology S.p.A
- ✓ ***Documentazione interna di riferimento***: Allianz Information Security Directives (AISD); Procedura Gestione e controllo degli accessi

3. Delitti di criminalità organizzata

3.1. La fattispecie di reato rilevante di cui all'art. 24-*ter*, D.lgs. 231/2001

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

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

Il reato associativo è caratterizzato, pertanto, dai seguenti elementi fondamentali: (i) *stabilità e permanenza*, poiché il vincolo associativo deve essere tendenzialmente stabile e destinato a durare anche oltre la realizzazione dei delitti concretamente programmati; (ii) *indeterminatezza del programma criminoso*, perché l'associazione a delinquere non si configura se i partecipanti si associano al fine di compiere un solo reato ma lo scopo dell'associazione deve essere quello di commettere più delitti, anche della stessa specie (in tal caso, l'indeterminatezza del programma criminoso riguarda l'entità numerica degli illeciti); (iii) *esistenza di una struttura organizzativa*, perché l'associazione deve prevedere una organizzazione di mezzi e di persone che, seppur in forma rudimentale, sia adeguata a realizzare il programma criminoso e a mettere in pericolo l'ordine pubblico.

In particolare, sono puniti coloro che promuovono, costituiscono o organizzano l'associazione, oltre a coloro che regolano l'attività collettiva da una posizione di superiorità o supremazia gerarchica. Sono altresì puniti con una pena inferiore tutti coloro che partecipano all'associazione.

Inoltre, ai sensi dell'art. 10 della legge 16 marzo 2006, n. 146, il reato in questione assume rilevanza ai fini della responsabilità amministrativa dell'ente anche se commesso a livello *transnazionale*. A tale riguardo, giova sottolineare che ai sensi dell'art. 3 della medesima legge si considera *transnazionale* il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché (i) sia commesso in più di uno Stato; ovvero (ii) sia commesso in uno Stato ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; ovvero (iii) sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; ovvero (iv) sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

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

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

Quanto, invece, ai reati non previsti espressamente dal D.lgs. 231/2001, nella giurisprudenza di legittimità si rinvengono orientamenti contrastanti circa una loro potenziale rilevanza. In una prima fase, infatti, la Corte di Cassazione sembrava escludere, sia pure ai soli fini dell'individuazione del profitto confiscabile, che reati non contemplati dal Decreto potessero dare rilevanza nella prospettiva di una loro imputazione quali delitti-scopo del reato associativo, in base al rilievo che in tal modo l'art. 416 c.p. (e il conseguente addebito di responsabilità nei confronti dell'ente *ex* art. 24-*ter* del Decreto) si sarebbe trasformato in una disposizione "aperta", in violazione del principio di tassatività del sistema sanzionatorio contemplato nel D.lgs. 231/2001 (in tal senso, Cass. pen., sez. VI, sent. 20 dicembre 2013, n. 3635).

Successivamente, però, sempre analizzando profili relativi alla corretta perimetrazione del profitto confiscabile in capo all'ente, sembra aver sposato una tesi meno restrittiva, riconoscendo la possibilità di ablazione di somme nei confronti della persona giuridica imputata – ai sensi dell'art. 24-*ter*, D.lgs. 231/2001 – sebbene i reati scopo del

sodalizio fossero illeciti di natura fiscale non contemplati tra quelli previsti dal Decreto (così, Cass. pen., sez. II, sent. 3 marzo 2017, n. 30255).

Orientamento, quest'ultimo, abbracciato – e precisato – anche da più recente sentenza (si tratta, in particolare, di Cass. pen., sez. III, sentenza 29 novembre 2019, n. 8785).

Ebbene, anche se astrattamente questo orientamento potrebbe portare a una "infinita" estensione della responsabilità amministrativa dell'ente, si noti, tuttavia, che dai repertori giurisprudenziali emerge come in tutti casi in cui è stato contestato all'ente l'art. 24-*ter* a fronte della commissione del reato di associazione per delinquere *ex* art. 416 c.p. finalizzato a reati-scopo estranei al catalogo del Decreto, gli stessi si sostanziavano in illeciti di natura tributaria, che, ora, sono invece contemplati tra i Reati Presupposto.

Esempio

Più Dirigenti e Dipendenti della Banca, d'intesa con uno o più Dirigenti della capogruppo Allianz SE e con il supporto di Consulenti legali all'uopo individuati, si associano allo scopo di commettere sistematiche violazioni della normativa tributaria italiana al fine di consentire alla Banca di non versare ingenti somme dovute a titolo di imposta.

3.2. Processi e attività sensibili rilevanti

In relazione ai delitti di criminalità organizzata, i Processi Sensibili della Banca potenzialmente più esposti al rischio di costituzione di una associazione per delinquere, fermi tutti gli altri presidi descritti negli altri capitoli della Parte Speciale del Modello in relazione ai vari possibili reati-scopo, sono:

- **II.** Gestione dei flussi monetari e finanziari;
- **III.** Selezione e gestione dei Consulenti finanziari;
- **VI.** Gestione dell'erogazione del credito;
- **VII.** Acquisto di beni, servizi e consulenze;
- **VIII.** Selezione, assunzione e gestione del personale.

Nello specifico, all'interno dei Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Selezione, assunzione e gestione del personale

- Processo Sensibile principale: **VIII**

b) Selezione delle controparti contrattuali, con particolare riferimento ai Fornitori e Consulenti;

- Processi Sensibili principali: **II** e **VII**

c) Selezione dei Consulenti finanziari abilitati all'offerta fuori sede;

- Processo Sensibile principale: **III**

d) Gestione dell'erogazione del credito

- Processo Sensibile principale: **VI**

3.3. Principi generali di comportamento

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, Consulenti Finanziari, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali, ai Fornitori e ai Consulenti nella misura necessaria alle funzioni dagli stessi svolte.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 24-*ter* del Decreto e di violare i principi e le procedure aziendali richiamate nella presente Parte Speciale.

Più nello specifico, nell'ambito di tale divieto di carattere generale e fermi tutti i divieti descritti negli altri capitoli della Parte Speciale del Modello in relazione ai vari possibili reati-scopo del reato di associazione per delinquere, è **proibito**:

- procedere alla assunzione di personale in azienda senza aver prima constatato la sussistenza dei requisiti di onorabilità e affidabilità;
- instaurare rapporti con soggetti terzi – persone fisiche o giuridiche, italiane o straniere – senza aver rispettato criteri e metodologie di selezione previsti dalle procedure aziendali che consentano di accertarne onorabilità e affidabilità;
- commercializzare prodotti bancari, finanziari, assicurativi attraverso canali distributivi non autorizzati dalla Banca.

3.4. Principi specifici per le singole attività sensibili

Con precipuo riferimento alle Attività Sensibili individuate *supra* § 3.2, fermi i divieti generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Selezione, assunzione e gestione del personale

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. h) della Parte Speciale)

b) Selezione delle controparti contrattuali, con particolare riferimento a Fornitori e Consulenti

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. g) della Parte Speciale)

c) Selezione dei consulenti finanziari abilitati all'offerta fuori sede

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. l) della Parte Speciale)

d) Gestione dell'erogazione del credito

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. k) della Parte Speciale)

4. Reati di contraffazione

4.1. Le fattispecie di reato rilevanti di cui all'art. 25-*bis* D.lgs. 231/2001

FALSIFICAZIONE DI MONETE, SPENDITA E INTRODUZIONE NELLO STATO, PREVIO CONCERTO, DI MONETE FALSIFICATE (ART. 453 C.P.)

La fattispecie di reato si realizza quando chiunque: 1) contraffà monete nazionali o straniere, aventi corso legale nello Stato o fuori; 2) altera in qualsiasi modo monete genuine, con il dare ad esse l'apparenza di un valore superiore; 3) introduce, non essendo concorso nella contraffazione o nell'alterazione, ma di concerto con chi l'ha eseguita ovvero con un intermediario, nel territorio dello Stato o detiene o spende o mette altrimenti in circolazione monete contraffatte o alterate; ovvero, 4) al fine di metterle in circolazione, acquista o comunque riceve, da chi le ha falsificate, ovvero da un intermediario, monete contraffatte o alterate.

Per *contraffazione* generalmente si intende la formazione integrale della cosa imitata, con notevole grado di fedeltà. Caratteristica principale della contraffazione è, pertanto, l'imitazione della cosa reale, l'apparenza di genuinità. L'*alterazione* ha, invece, come presupposto l'esistenza di una moneta genuina e la sua circolazione legale costante e consiste, attraverso la manomissione, in una modificazione della sostanza o delle caratteristiche formali della moneta, tale da alterarne il valore.

Nella fattispecie di cui all'art. 453 c.p. il legislatore ha inteso punire sia il soggetto che pone in essere la contraffazione o l'alterazione sia colui che, in concerto con chi abbia proceduto alla contraffazione o alterazione o con un suo intermediario, metta in circolazione in qualsiasi modo le monete così contraffatte o alterate sia, infine, colui che, al fine di metterle in circolazione, le procuri presso il soggetto che le ha contraffatte o alterate o presso un suo intermediario.

Esempio

Un Dipendente della Banca, d'intesa con un cliente, mette in circolazione banconote contraffatte.

SPENDITA E INTRODUZIONE NELLO STATO, SENZA CONCERTO, DI MONETE FALSIFICATE (ART. 455 C.P.)

Il reato si perfeziona quando chiunque, fuori dai casi previsti dagli artt. 453 e 454 c.p., introduce nel territorio dello Stato, acquista o detiene monete contraffatte o alterate, al fine di metterle in circolazione ovvero le spende o le mette altrimenti in circolazione, per cui l'ipotesi di reato qui contemplata viene ad avere carattere residuale nel senso che presuppone almeno la consapevolezza o l'iniziale sospetto della non autenticità delle monete, pur in assenza di qualunque accordo con il soggetto che abbia materialmente compiuto la falsificazione.

Esempio

Un Dipendente della Banca introduce nel territorio dello Stato delle monete contraffatte, mettendole poi in circolazione.

SPENDITA DI MONETE FALSIFICATE RICEVUTE IN BUONA FEDE (ART. 457 C.P.)

Il reato di cui all'art. 457 c.p. punisce chiunque spende, o mette in circolazione monete contraffatte o alterate, da lui ricevute in buona fede.

Il reato richiede che l'agente abbia ricevuto le monete contraffatte in buona fede e quindi le abbia successivamente fatte circolare. Affinché possa dirsi integrato il reato in esame è comunque necessario che l'agente al momento della spendita o della messa in circolazione fosse consapevole della falsità.

Il bene giuridico tutelato dalle norme che puniscono il falso nummario è la pubblica fede che viene messa in pericolo da condotte che possono pregiudicare il sentimento di fiducia generalizzata nei confronti dell'autenticità dei mezzi di scambio.

Esempio

Un funzionario della Banca riceve in buona fede da un cliente delle banconote contraffatte e, nonostante sia venuto successivamente conoscenza della loro falsità, le mette in circolazione.

CONTRAFFAZIONE, ALTERAZIONE O USO DI MARCHI O SEGNI DISTINTIVI OVVERO DI BREVETTI, MODELLI E DISEGNI (ART. 473 C.P.)

L'art. 473 c.p. sanziona penalmente chiunque (a) potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali; (b) contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati. La norma tutela la fiducia che il pubblico ha nella genuinità dei segni distintivi di prodotti industriali, ossia, soprattutto, di (i) *marchi*, ossia segni (emblema, figura, denominazione, ecc.) destinati a distinguere merci o prodotti di una determinata impresa; (ii) *brevetti*, ovvero attestati con i quali è concesso il diritto all'uso esclusivo di una invenzione o scoperta.

La condotta viene penalmente sanzionata anche nel caso di utilizzo commerciale o industriale dei marchi o dei segni distintivi già contraffatti.

Esempio

Un Dipendente della Banca deve promuovere un nuovo prodotto finanziario per la Società, già adottato da un competitor molto rilevante sul mercato e, per questo motivo, decide di usufruire di un nome e di un simbolo molto simili a quelli utilizzati per il prodotto promosso dalla banca concorrente.

4.2. Processi e attività sensibili rilevanti

In relazione ai delitti contro l'industria e il commercio e i reati di contraffazione, il Processo Sensibile della Banca potenzialmente più esposto alle fattispecie di Reato ritenute rilevanti sopra richiamata, è:

- **II.** Gestione dei flussi monetari e finanziari;
- **V.** Commercializzazione dei prodotti bancari, finanziari e assicurativi.

Nello specifico, all'interno dei Processo Sensibili, sono state individuate la seguenti Attività Sensibili:

a) Commercializzazione dei prodotti bancari, finanziari e assicurativi nonché dei servizi fiduciari;

- Processi Sensibili principali: **II** e **V**

b) Gestione dei servizi di trasporto, custodia e contazione del contante;

- Processi Sensibili principali: **II** e **V**

c) Operazioni disposte dalla clientela.

- Processo Sensibile principale: **V**

4.3. Principi generali di comportamento

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti, membri degli Organi sociali della Banca, ai Consulenti Finanziari, nonché ai Consulenti nella misura necessaria alle attività dagli stessi svolte.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*bis* del Decreto e di violare i principi e le procedure aziendali richiamate nella presente Parte Speciale.

Più nello specifico, nell'ambito di tale divieto di carattere generale, è **proibito**:

- contraffare o alterare monete nazionali o straniere o comunque mettere in circolazione o spendere monete nazionali o straniere contraffatte o alterate;
- usare nomi o segni distintivi per la commercializzazione dei prodotti bancari, finanziari e assicurativi della Banca che siano idonei a produrre confusione con nomi o segni distintivi legittimamente usati da altre banche o compagnie;
- utilizzare marchi diversi da quelli espressamente autorizzati dalla Banca per la commercializzazione dei prodotti bancari, finanziari e assicurativi;
- imitare servilmente i prodotti di un concorrente che abbiano caratteristiche peculiari e specifiche tali da poter essere considerate proteggibili dalla normativa in oggetto;
- effettuare una descrizione di un prodotto finanziario, bancario o assicurativo non esattamente corrispondente a quella reale;
- diffondere notizie e/o apprezzamenti sui prodotti e sull'attività di un concorrente che siano anche solo potenzialmente idonei a determinarne il discredito;
- partecipare a gare o a *beauty contest* qualora tale attività non rientri nella propria *job description* ovvero, in tale ultima ipotesi, senza preventiva autorizzazione da parte delle funzioni competenti;
- effettuare qualsiasi attività che possa essere considerata una forma di concorrenza non pienamente corretta e trasparente.

4.4. Principi specifici per l'attività sensibile

Con precipuo riferimento alle Attività Sensibili individuate *supra* § 4.2, fermi i divieti generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Commercializzazione di prodotti bancari, finanziari e assicurativi, nonché servizi fiduciari

i La Banca predispone presidi volti ad accertare l'inconfondibilità dei segni distintivi utilizzati per commercializzare e pubblicizzare prodotti bancari, finanziari e assicurativi;

ii La Banca prevede, all'interno delle procedure relative allo sviluppo e alla commercializzazione dei prodotti assicurativi, un processo di consultazione delle banche dati messe a disposizione dall'Ufficio Italiano Marchi e Brevetti da attuarsi ogni volta che si intendano utilizzare nuovi segni o simboli grafici;

iii La Banca adotta presidi attraverso i quali verificare la corretta e fedele descrizione dei prodotti bancari, finanziari e assicurativi lanciati sul mercato;

iv La Banca verifica i parametri necessari per la valutazione di adeguatezza e appropriatezza cui deve esser sottoposto il prodotto.

- ✓ ***Control Owner****:* Unità organizzativa Organizzazione e Sviluppo applicativo; Unità Organizzativa Communication, Digitali & Personal Marketing
- ✓ ***Documentazione interna di riferimento***: Procedura Approvazione e lancio di un nuovo prodotto

v La Banca attua una procedura volta a definire le modalità di gestione dell'attività di approvazione, sviluppo e modifica dei prodotti. All'interno della suddetta procedura sono delineate le analisi e le verifiche della funzione Compliance e Antiriciclaggio sulla conformità del prodotto rispetto alla normativa applicabile;

- ✓ ***Control Owner****:* Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Approvazione e lancio di un nuovo prodotto

vi. La Banca predispone controlli periodici sui contenuti del sito internet, delle brochure pubblicitarie e su altri eventuali supporti informatici o cartacei attraverso i quali sono commercializzati e/o pubblicizzati i prodotti bancari, finanziari e assicurativi;

- ✓ ***Control Owner****:* Unità Organizzativa Communication, Digitali & Personal Marketing
- ✓ ***Documentazione interna di riferimento***: Procedura Approvazione e lancio di un nuovo prodotto

vii. Il Consulente Finanziario, nello svolgimento della sua attività, è tenuto a comportarsi in modo onesto, leale e corretto evitando azioni e comportamenti riconducibili a fenomeni di miss-selling (e.g. rappresentazione non chiara e corretta dei prodotti o servizi e relativi costi e rischi finanziari al cliente);

- ✓ ***Control Owner****:* Organismo di vigilanza e tenuta dell'albo unico dei Consulenti Finanziari
- ✓ ***Documentazione interna di riferimento***: Procedura Obblighi del Consulente finanziario abilitato all'offerta fuori Sede; Procedura Distribuzione di prodotti e servizi da parte della rete dei Consulenti finanziari abilitati all'offerta fuori Sede

viii. La Banca attua una procedura volta a definire le modalità operative messe in atto per la redazione e l'aggiornamento del Manuale provvigionale ed operativo per i Consulenti Finanziari abilitati all'offerta fuori sede legata al collocamento del nuovo prodotto;

- ✓ ***Control Owner****:* Unità organizzativa Pianificazione Commerciale
- ✓ ***Documentazione interna di riferimento***: Procedura Approvazione e lancio di un nuovo prodotto

ix. La Banca, nel caso di utilizzo di marchio di Società terze, provvede a verificare l'eventuale esigenza di richiedere la preventiva autorizzazione alle case prodotto con cui la Banca ha stipulato accordi di collocamento per l'utilizzo del marchio e/o di loghi, senza la quale non si può procedere alla pubblicazione della comunicazione;

- ✓ ***Control Owner****:* Unità organizzativa Fondi e Sicav
- ✓ ***Documentazione interna di riferimento***: Procedura Comunicazioni pubblicitarie e promozionali

b) Gestione dei servizi di trasporto, custodia e contazione del contante

i. Qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dei servizi di trasporto, custodia e contazione del denaro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.lgs. 231/2001 e di impegno al suo rispetto;

- ✓ ***Control Owner****:* Unità Organizzativa Consulenza Legale Banca
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

ii. La Società incaricata, nel caso in cui vi sia necessità, preleva il contante unicamente dalle riserve presenti presso la Banca d'Italia al fine di garantire che tutto il contante utilizzato dalla Banca sia certificato da Banca d'Italia;

- ✓ ***Control Owner****:* Direzione Operativa
- ✓ ***Documentazione interna di riferimento***: Procedura Approvvigionamento di denaro contante

iii. La Banca si è dotata di una *Policy* di esternalizzazione di funzioni aziendali nella quale sono disciplinate tutte le fasi in cui si articola il processo di esternalizzazione e di un processo che prevede l'*iter* operativo in caso si decida di esternalizzare una funzione;

- ✓ ***Control Owner****:* Direzione Compliance & Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Policy di esternalizzazione di funzioni aziendali

iv. Quotidianamente, e comunque ogni qualvolta sia necessario, l'addetto della filiale incaricata provvede ad aggiornare uno specifico foglio di lavoro *excel* utilizzato per monitorare l'operato dell'*outsourcer*, anche con particolare riferimento ai livelli di servizio (c.d. SLA) e di performance (c.d. KPI) previsti all'interno del contratto;

- ✓ ***Control Owner**:* Responsabile Direzione Risorse in qualità del Referente della Funzione Esternalizzata
- ✓ ***Documentazione interna di riferimento***: Procedura Approvvigionamento di denaro contante; Policy di esternalizzazione di funzioni aziendali

v. Il Responsabile della funzione preposta, provvede ad effettuare specifiche visite in loco presso la sede centrale dell'*outsourcer* incaricato. In particolare, nell'ambito di tali verifiche, vengono effettuate le seguenti attività di controllo: (i) conta fisica delle giacenze; (ii) verifica delle condizioni dei locali; (iii) verifica dei presidi adottati al fine di garantire la sicurezza; (iv) presa visione delle banconote di pertinenza della Banca classificate come "logore" eventualmente ancora presenti presso i locali dell'*outsourcer*.

- ✓ ***Control Owner**:* Responsabile dell'Unità Organizzativa Call Center e Sportelli
- ✓ ***Documentazione interna di riferimento***: Procedura Approvvigionamento di denaro contante

vi. Con cadenza almeno annuale, il Responsabile della funzione preposta ai controlli predispone un apposito *report* contente: (i) le risultanze ottenute dalle attività di monitoraggio effettuate; (ii) eventuali ulteriori statistiche relative ai livelli di servizio forniti dall'*outsourcer*; (iii) una valutazione sintetica e complessiva dell'operato dell'*outsourcer*.

- ✓ ***Control Owner**:* Responsabile dell'Unità Organizzativa Call Center e Sportelli
- ✓ ***Documentazione interna di riferimento***: Procedura Approvvigionamento di denaro contante; Policy di esternalizzazione di funzioni aziendali

c) Esecuzione di operazioni disposte dalla clientela

i La Banca prevede l'utilizzo di apparecchiature per l'autenticazione e la selezione delle banconote conformi alle predette disposizioni e soggette ad aggiornamento periodico del *software*;

ii La Banca prevede programmi di formazione del personale sia su aspetti normativi che tecnici connessi all'attività di trattamento del contante; è inoltre previsto l'obbligo di ritiro dalla circolazione di banconote e monete sospette di falsità;

iii Nel caso di malfunzionamento della macchina conta banconote, è cura dell'addetto di filiale stesso procedere direttamente all'esame manuale delle banconote sulla base degli *standard* di autenticità definiti per le banconote in Euro;

iv La Banca ha definito i comportamenti da attuare in caso di rilevazione di banconote o monete sospette di falsità;

v La Banca invia tempestivamente alle filiali della Banca d'Italia delle banconote e monete che non hanno superato i controlli.

- ✓ ***Control Owner**:* Responsabile Direzione Operativa
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione banconote sospette di falsità e logore

5. Reati societari

5.1. Le fattispecie di reato rilevanti di cui all'art. 25-*ter*, D.lgs. 231/2001

FALSE COMUNICAZIONI SOCIALI (ART. 2621 C.C.)

FALSE COMUNICAZIONI SOCIALI NELLE SOCIETÀ QUOTATE (ART. 2622 C.C.)

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

Si precisa che: (**i**) le informazioni false o omesse devono essere tali da alterare la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene; (**ii**) la stessa pena si applica se le falsità o le omissioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

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

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

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

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

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

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

Esempio

Gli Amministratori redigono un bilancio indicando nelle poste attive crediti in realtà inesistenti, al fine di conseguire un ingiusto profitto per la Banca.

IMPEDITO CONTROLLO (ART. 2625, CO. 2, C.C.)

Il reato di impedito controllo si verifica nell'ipotesi in cui, mediante l'occultamento di documenti o altri artifici idonei allo scopo, gli amministratori impediscono o, più semplicemente, ostacolano lo svolgimento delle attività di controllo attribuite dalla legge ai soci o ad altri organi sociali.

Il reato è presupposto della responsabilità degli enti nella sola ipotesi in cui l'impedimento o il semplice ostacolo creato dagli amministratori abbia procurato un danno ai soci, stante l'esplicito riferimento nel Decreto al solo secondo comma della disposizione in esame.

Esempio

Un Amministratore della Banca occulta documenti al Collegio Sindacale, ostacolandone l'attività di controllo e, così, cagionando un danno ai soci.

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

La condotta tipica del reato previsto dall'art. 2626 c.c. prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione da parte degli amministratori, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

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

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

Esempio

Gli Amministratori, fuori dai casi di legittima riduzione del capitale sociale, liberano i soci dall'obbligo di eseguire i conferimenti dovuti.

ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE (ART. 2627 C.C.)

Il reato di illegale ripartizione di utili e riserve *ex* art. 2627 c.c. contempla due distinte ipotesi: in primo luogo, quella in cui si ripartiscano utili, o acconti sugli utili, che non siano stati effettivamente conseguiti, o che siano destinati per legge a riserva; in secondo luogo, quella in cui si ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Il bene giuridico tutelato dalla norma deve essere identificato nell'integrità del capitale sociale reale e delle riserve obbligatorie relativamente alla fase di esercizio dell'attività di impresa. Secondo la dottrina, il riferimento agli «*utili*» contenuto nella disposizione va letto come riferimento al concetto di utile di bilancio, inteso quale risultato complessivo dell'attività economica della società in cui rientrino anche gli incrementi patrimoniali derivanti da operazioni occasionali o comunque diverse rispetto a quelle tipiche dell'oggetto sociale. Qualora gli utili siano restituiti, o le riserve ricostituite, prima del termine per l'approvazione del bilancio, il reato si estingue.

Esempio

Il Consiglio di Amministrazione della Banca delibera la distribuzione di dividendi che costituiscono non un utile di esercizio ma fondi non distribuibili perché destinati dalla legge a riserva legale.

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

Il reato in questione si perfeziona con l'acquisto o la sottoscrizione, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della società controllante, in modo tale da procurare una lesione all'integrità del capitale sociale e delle riserve non distribuibili per legge. Soggetti attivi del reato sono gli amministratori.

Tuttavia, la ricostituzione del capitale sociale o delle riserve prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio nel corso del quale è stata posta in essere la condotta, estingue il reato.

I casi e i limiti per l'acquisto di azioni proprie da parte della società, cui si riferisce l'art. 2628 c.c., sono stabiliti dal codice civile e dalla legislazione sugli emittenti. Il codice civile disciplina altresì i limiti temporali e contenutistici per l'acquisto di azioni proprie da parte dei consiglieri a ciò delegati.

Esempio

*Il Consiglio di Amministrazione procede all'acquisto o alla sottoscrizione di azioni della Banca fuori dai casi di cui all'art. 2357 c.c. o di una società controllante fuori dai casi di cui all'art. 2359-*bis *c.c., cagionando in tal modo una lesione del patrimonio sociale.*

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

Il reato si realizza nell'ipotesi in cui si proceda a riduzioni del capitale sociale, a fusioni con altra società ovvero a scissioni della società stessa, in violazione delle disposizioni previste dalla legge a tutela dei creditori. Perché il reato

sussista, tuttavia, è necessario che da tali operazioni derivi un pregiudizio ai creditori; il reato si estingue qualora i creditori danneggiati siano risarciti prima del giudizio.

Esempio

Il Consiglio di Amministrazione delibera la riduzione del capitale sociale in violazione delle disposizioni di legge, cagionando un pregiudizio ai creditori della medesima.

OMESSA COMUNICAZIONE DEL CONFLITTO DI INTERESSI (ART. 2629-*BIS* C.C.)

La condotta criminosa consiste nella violazione degli obblighi imposti dall'art. 2391, co. 1, c.c., il quale prevede che l'amministratore debba dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata; e che, se si tratti di amministratore delegato, debba altresì dal compiere l'operazione, investendo della stessa l'organo collegiale, mentre se si tratta di amministratore unico debba darne notizia alla prima assemblea utile.

Ai fini della sussistenza del reato, è necessario che la condotta abbia cagionato un danno alla società o a terzi.

L'art. 2629-*bis* c.c., inoltre, si applica solo agli amministratori o ai componenti del consiglio di gestione di «*una società con titoli quotati in mercato regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209, o del decreto legislativo 21 aprile 1993, n. 124*».

Esempio

Un Amministratore della Banca non dà notizia agli altri Amministratori e/o al Collegio Sindacale che ha un interesse in conflitto in una operazione di acquisizione societaria intrapresa da Allianz Bank nei confronti della società di un suo fratello, in modo da garantire un vantaggio economico al parente.

FORMAZIONE FITTIZIA DEL CAPITALE SOCIALE (ART. 2632 C.C.)

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

Esempio

La Banca delibera un aumento di capitale che viene interamente sottoscritto da Allianz S.p.A. che, a sua volta, delibera un aumento del proprio capitale questa volta sottoscritto interamente da Allianz Bank.

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

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

Il reato di corruzione tra privati, profondamente modificato dal decreto legislativo 15 marzo 2017, n. 38, punisce, salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà. Ai sensi del

medesimo comma, poi, è parimenti sanzionato chi, nell'ambito organizzativo della società o dell'ente privato, «*esercita funzioni direttive diverse*» rispetto a quelle indicate.

Inoltre, l'art. 2635, co. 2, c.c. punisce – con una pena inferiore – gli stessi fatti se commessi «*da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati dal primo comma*».

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

Nel codice civile è stato inoltre introdotto il reato di istigazione alla corruzione tra privati (art. 2635-*bis* c.c.): a questo proposito, la condotta rilevante ai sensi del Decreto si realizza attraverso l'offerta o la promessa di denaro o altra utilità non dovuti ai soggetti apicali o aventi funzioni direttive in società o enti privati, affinché questi ultimi compiano od omettano atti in violazione degli obblighi inerenti all'ufficio o degli obblighi di fedeltà, quando l'offerta o la promessa non sia accettata.

Merita segnalare, infine, che la L. 3/2019 ha modificato il regime di procedibilità a querela sia della corruzione tra privati che dell'istigazione alla corruzione tra privati, prevedendo per entrambe la procedibilità d'ufficio.

Esempio

Un Dirigente della Banca offre denaro al responsabile commerciale di un'altra società al fine di sottoscrivere un contratto a condizioni più favorevoli rispetto a quelle di mercato.

Un Dirigente della Banca offre denaro al responsabile commerciale di un'altra società al fine di sottoscrivere un contratto a condizioni più favorevoli rispetto a quelle di mercato, ma l'offerta non viene accettata.

ILLECITA INFLUENZA SULL'ASSEMBLEA (ART. 2636 C.C.)

Il reato si perfeziona attraverso il compimento di atti simulati o fraudolenti, da chiunque posti in essere e a prescindere dalla finalità perseguita, che abbiano quale effetto la formazione di una maggioranza artificiosa all'interno dell'assemblea sociale.

Esempio

Uno o più Amministratori falsificano documentazione al fine di influenzare illecitamente una delibera assembleare.

AGGIOTAGGIO (ART. 2637 C.C.)

Richiamato dall'art. 25-*ter*, lett. s), D.lgs. 231/2001 il reato verrà analizzato, per analogia di materia, nel capitolo di Parte Speciale dedicato agli abusi di mercato (§8).

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

Tale reato è posto a tutela delle funzioni di controllo esterno della società e si realizza in due diverse ipotesi.

La prima ipotesi, che punisce le false informazioni alle Autorità di vigilanza, si configura nel caso in cui soggetti dotati di una particolare qualifica (amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci, liquidatori di società o enti e, in generale, altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti) espongano, nelle comunicazioni obbligatorie per legge alle Autorità di Vigilanza, fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, ovvero occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che erano tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi. In tale prima ipotesi, quindi, il reato si perfeziona nel caso in cui la condotta criminosa sia specificamente volta a ostacolare l'attività delle Autorità di vigilanza.

La seconda ipotesi, che si focalizza sulla realizzazione di un ostacolo alle funzioni di vigilanza, si configura indipendentemente dalle peculiarità della condotta e dal fine perseguito dagli agenti: rileva esclusivamente che l'attività dell'Autorità di vigilanza sia stata ostacolata dalla condotta – qualunque essa sia – dell'agente.

Esempio

L'Amministratore Delegato della Banca omette di comunicare alle Autorità di vigilanza competenti l'acquisizione di una partecipazione rilevante, al fine di evitare i controlli delle stesse Autorità.

5.2. Processi e attività sensibili rilevanti

In relazione ai Reati societari sino a qui descritti, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

I. Gestione degli adempimenti e dei rapporti con gli enti pubblici e le autorità amministrative indipendenti, anche in occasione di verifiche ispettive;

II. Gestione dei flussi monetari e finanziari;

III. Selezione e gestione dei consulenti finanziari;

IV. Formazione del bilancio e gestione degli adempimenti societari e dei rapporti con gli organi di controllo;

V. Commercializzazione dei prodotti bancari, finanziari e assicurativi;

VI. Gestione dell'erogazione del credito;

VII. Acquisto di beni, servizi e consulenze;

VIII. Selezione, assunzione e gestione del personale;

IX. Gestione di omaggi, delle sponsorizzazioni e altre liberalità;

X. Gestione del contenzioso;

XII. Gestione dei rapporti con i *media* e delle informazioni privilegiate.

Nello specifico, all'interno dei singoli Processi Sensibili, in relazione a tutti i Reati societari sopra richiamati al netto delle fattispecie di cui agli artt. 2635 e 2635-*bis* c.c., sono state individuate le seguenti Attività Sensibili:

a) Gestione delle comunicazioni esterne, con particolare riferimento alle comunicazioni rivolte alle Autorità di vigilanza e alle altre comunicazioni sociali previste dalla legge dirette ai soci o al pubblico (*e.g.*, informazioni relative ai bilanci e relazioni riguardanti la situazione economica, patrimoniale e finanziaria della Banca e del Gruppo al quale essa appartiene);

- Processo Sensibile principale: **IV**

b) Tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni delle Autorità di vigilanza;

- Processo Sensibile principale: **IV**

c) Gestione degli adempimenti e dei rapporti con le Autorità di vigilanza in occasione di verifiche, ispezioni e accertamenti;

- Processo Sensibile principale: **I**

d) Gestione dei rapporti con il Collegio Sindacale, la società di revisione e gli altri organi societari, nonché redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il loro controllo;

- Processo Sensibile principale: **IV**

e) Gestione delle operazioni di incremento o riduzione del capitale sociale o di altre operazioni su azioni o quote sociali, nonché operazioni di ripartizione degli utili di esercizio, delle riserve e di restituzione dei conferimenti;

- Processo Sensibile principale: **IV**

f) Approvazione delle delibere consiliari aventi a oggetto operazioni in relazione alle quali gli Amministratori siano portatori di un interesse diverso da quello della Società;

- Processo Sensibile principale: **IV**

g) Predisposizione della documentazione che sarà oggetto di discussione e di delibera in Assemblea dei Soci e gestione dei rapporti con tale Organo sociale.

- Processo Sensibile principale: **IV**

In relazione alla peculiarità che caratterizzano i reati di corruzione tra privati (art. 2635 c.c.) e di istigazione alla corruzione tra privati (art. 2635-*bis* c.c.), sono state inoltre individuate le seguenti Attività Sensibili potenzialmente rischiose:

h) Commercializzazione dei prodotti bancari, finanziari e assicurativi, nonché servizi fiduciari;

- Processo Sensibile principale: **V**

i) Gestione dell'erogazione del credito;

- Processo Sensibile principale: **VI**

j) Acquisto di beni, servizi e consulenze;

- Processi Sensibili principali: **II** e **VII**

k) Partecipazione a gare d'appalto;

- Processo Sensibile principale: **V**

l) Rapporti con i *media*;

- Processo Sensibile principale: **XII**

m) Gestione delle controversie e accordi transattivi;

- Processo Sensibile principale: **X**

n) Gestione degli omaggi, liberalità nonché delle spese di rappresentanza;

- Processi Sensibili principali: **II** e **IX**

o) Selezione, assunzione e gestione del personale;

- Processo Sensibile principale: **VIII**

p) Selezione dei Consulenti Finanziai abilitati all'offerta fuori sede;

- Processo Sensibile principale: **III**

q) Provvigioni e incentivi ai Consulenti Finanziari abilitati all'offerta fuori sede;

- Processo Sensibile principale: **III**

r) Gestione delle sponsorizzazioni e delle donazioni;

- Processo Sensibile principale: **II** e **IX**

s) Gestione dei servizi di trasporto, custodia e contazione del contante;

- Processo Sensibile principale: **V**

5.3. Principi generali di comportamento

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, Consulenti Finanziari, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali, ai Consulenti e ai Fornitori.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*ter* del Decreto e di violare i principi e le procedure aziendali richiamate nella presente Parte Speciale.

Più nello specifico, nelle attività di predisposizione del bilancio e delle altre comunicazioni sociali, nonché in tutte le altre attività o operazioni che potrebbero avere un riflesso sul patrimonio della Banca o sulle garanzie creditorie, è **proibito**:

- esporre nei bilanci, nelle relazioni e in tutte le altre comunicazioni sociali previste dalla legge, fatti materiali non rispondenti al vero, ovvero omettere fatti materiali la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale e finanziaria Gruppo o del Gruppo bancario;
- alterare i dati e le informazioni destinate alla predisposizione dei prospetti informativi predisposti dalla Banca o dalla Capogruppo Allianz;
- illustrare i dati e le informazioni utilizzate in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria del Gruppo e del Gruppo Bancario, sull'evoluzione della sua attività, nonché sugli strumenti finanziari e sui relativi diritti;
- impedire, in qualsiasi modo, le attività di controllo legalmente attribuito al Collegio Sindacale;
- restituire conferimenti ai soci (o liberare gli stessi dall'obbligo di eseguirli) fuori dai casi previsti dalla legge;
- compiere operazioni di ripartizione di utili o di riserve fuori dai casi consentiti dalle legge;
- compiere qualsiasi operazione che possa aumentare in modo fittizio il capitale sociale o che, comunque, possa cagionare un danno ai creditori della Banca;
- omettere, qualora si rivesta la qualifica di Consigliere di Amministrazione, di comunicare al Consiglio di Amministrazione un interesse in conflitto con quello della Banca;
- pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento od ingannatorio aventi ad oggetto strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato ed idonei ad alterarne sensibilmente il prezzo.

Ancora, nelle attività di gestione degli adempimenti amministrativi della Banca e di gestione dei rapporti e delle comunicazioni nei confronti delle Autorità di vigilanza, è **proibito**:

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

- esporre fatti materiali non veritieri, ancorché di carattere valutativo, nelle comunicazioni obbligatorie per legge, ovvero occultare con mezzi fraudolenti, in tutto o in parte, fatti – di cui è obbligatoria la comunicazione – sulla situazione patrimoniale, economica o finanziaria della Banca;
- occultare, nel corso di verifiche, ispezioni, o accessi di funzionari delle Autorità di vigilanza, documenti, relazioni o atti di cui è stata richiesta l'esibizione;
- comunque, ostacolare in qualsiasi altra forma le funzioni di controllo delle Autorità di vigilanza.

Da ultimo, nella gestione delle attività bancarie, in quella di gestione degli investimenti e in tutti i rapporti con soggetti privati che, per qualsiasi ragione, vengono a contatto con le attività della Società, è **proibito**:

- effettuare pagamenti in contanti;
- offrire, promettere, corrispondere indebitamente, nell'esercizio dell'attività aziendale, anche in via indiretta, denaro o comunque cose di valore a favore di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili, sindaci, liquidatori, dipendenti e collaboratori a qualsiasi titolo di società o consorzi;
- promettere o accordare vantaggi di qualsiasi natura (come, p.e., promesse di assunzione), anche in via indiretta, in favore di persone giuridiche o fisiche (inclusi i familiari di esponenti di aziende con cui la Banca ha in corso – o intende intrattenere – rapporti commerciali o inerenti la gestione del *business* aziendale), rivolti ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale o che possano comunque influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;
- promettere, offrire, donare (o autorizzare la donazione di) regali o promettere, offrire, concedere (o autorizzare la concessione di) inviti ad eventi, anche in via indiretta, al di fuori di quanto previsto dalle *policy* aziendali e di Gruppo;
- effettuare prestazioni in favore dei Consulenti, Consulenti finanziari abilitati all'offerta fuori sede, *Partner* che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi o riconoscere compensi in favore dei medesimi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti nel settore;
- effettuare atti di liberalità o sponsorizzazioni senza rispettare i principi di trasparenza imposti dalle *policy* aziendali e di Gruppo;
- instaurare *partnership*, *joint venture*, altre forme di rapporti commerciali (come, p.e., rapporti di intermediazione, rapporti di consulenza, ecc.) e rapporti di lavoro, anche dipendente, con soggetti terzi senza aver preventivamente effettuato una verifica dell'attendibilità ed onorabilità degli stessi.

5.4. Principi specifici per le singole attività sensibili

Con precipuo riferimento alle Attività Sensibili individuate *supra* § 5.2, fermi i divieti generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Gestione delle comunicazioni esterne, con particolare riferimento alle comunicazioni alle Autorità di vigilanza e alle altre comunicazioni sociali previste dalla legge dirette ai soci o al pubblico; e

b) Tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di Autorità di Vigilanza

i Con riferimento alle attività della società soggette alla vigilanza di pubbliche autorità, in base alle specifiche normative applicabili e al fine di prevenire la commissione del reato di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, le comunicazioni devono essere svolte in base alle

procedure aziendali esistenti, contenenti la disciplina delle modalità e l'attribuzione di specifiche responsabilità in relazione: (i) predisposizione e invio delle segnalazioni periodiche alle Autorità previste da leggi e regolamenti; (ii) predisposizione e trasmissione a queste ultime dei documenti previsti in leggi e regolamenti (ad es., bilanci e verbali delle riunioni degli Organi Sociali); (iii) predisposizione e trasmissione di dati e documenti specificamente richiesti dalle Autorità di vigilanza; (iv) al comportamento da tenere nel corso degli accertamenti ispettivi;

ii La Banca deve garantire un'adeguata formalizzazione delle procedure in oggetto e successiva documentazione dell'esecuzione degli adempimenti in esse previsti, con particolare riferimento all'attività di elaborazione dei dati;

- ✓ ***Control Owner*****:** Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con le Autorità di Vigilanza; Procedura Comunicazioni alle Autorità di Vigilanza e ad altri Enti esterni; Procedura Gestione richieste dalle Autorità giudiziarie e da Agenzia Entrate

iii Le comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Banca devono essere redatte in base alle specifiche procedure aziendali in essere che: (i) determinano con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili; (ii) prevedono la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema (anche informatico) che consente la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema; (iii) prevedono criteri e modalità per l'elaborazione dei dati del bilancio consolidato e la trasmissione degli stessi da parte delle società rientranti nel perimetro di consolidamento;

- ✓ ***Control Owner***: Direzione Finanza Amministrazione e Controllo
- ✓ ***Documentazione interna di riferimento***: Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Reporting a Controllante e Capogruppo; Procedura Predisposizione situazioni periodiche

iv La Banca attua tutti gli interventi di natura organizzativo-contabile necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni ed il loro puntuale invio all'Autorità di vigilanza, secondo le modalità ed i tempi stabiliti dalla normativa applicabile;

- ✓ ***Control Owner***: Unità Organizzativa Contabilità e Bilancio; Unità Organizzativa Vigilanza e Reporting
- ✓ ***Documentazione interna di riferimento***: Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Reporting a Controllante e Capogruppo; Procedura Predisposizione situazioni periodiche

v Il Responsabile dell'Unità Organizzativa Amministrazione, competente alla rilevazione dei dati di bilancio e alla loro elaborazione ai fini della predisposizione della bozza di bilancio, rilascia un'apposita dichiarazione, attestante: (i) veridicità, correttezza, precisione e completezza di dati e informazioni contenute nel bilancio ovvero negli altri documenti contabili e nei documenti a questi ultimi connessi; (ii) la mancanza di elementi o dati che possano ingenerare il dubbio che le dichiarazioni e i dati raccolti contengano elementi incompleti o inesatti; (iii) predisposizione di un adeguato sistema di controllo teso a fornire una ragionevole certezza sui dati di bilancio; (iv) il rispetto delle procedure previste. La dichiarazione, deve essere presentata al Consiglio di Amministrazione in occasione della delibera di approvazione del proprio progetto di bilancio civilistico. Il Responsabile dell'Unità Organizzativa Amministrazione e dell' Unità Organizzativa Vigilanza e Reporting predispongono periodicamente una nota operativa per la definizione di contenuti e tempistica della predisposizione del progetto di bilancio di esercizio, nonché degli altri documenti contabili sopra indicati. La Banca prevede idonea attività di

formazione e aggiornamento rivolta alle funzioni coinvolte nella predisposizione dei documenti indicati nel presente paragrafo, con il supporto della Direzione Risorse;

- ✓ ***Control Owner*:** Responsabile dell'Unità Organizzativa Amministrazione; Unità Organizzativa Vigilanza e Reporting; Unità Direzione Risorse per l'erogazione delle attività formative
- ✓ ***Documentazione interna di riferimento:*** Procedura Tenuta della contabilità generale; Procedura Tenuta libri contabili obbligatori; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Reporting a Controllante e Capogruppo; Procedura Predisposizione situazioni periodiche; Procedura Formazione del personale; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma

c) Gestione degli adempimenti e dei rapporti con le Autorità di vigilanza in occasione di verifiche, ispezioni ed accertamenti

i Nel corso di verifiche, ispezioni o accertamenti deve essere prestata da parte delle funzioni e delle articolazioni organizzative ispezionate la massima collaborazione all'espletamento delle attività. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di interloquire con l'Autorità di vigilanza.

ii La Banca identifica il personale incaricato alla gestione dei rapporti con la Pubblica Amministrazione nel caso di visite ispettive, con indicazione dei compiti, ruoli, e responsabilità in accordo con la stratificazione dei poteri delegati;

iii La Banca definisce e formalizza i compiti e i comportamenti da adottare nel corso di eventuali visite ispettive e archivia i verbali predisposti a seguito delle stesse;

iv L'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della direzione o unità organizzativa aziendale di volta in volta interessata. Di tutto il processo relativo all'ispezione, al fine di garantire massima tracciabilità delle informazioni fornite, devono essere redatti appositi verbali, che verranno conservati dall'Organismo.

- ✓ ***Control Owner*:** Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con le Autorità di Vigilanza; Procedura Gestione richieste dalle Autorità giudiziarie e da Agenzia Entrate

d) Gestione dei rapporti con il Collegio Sindacale, la società di revisione e gli altri organi societari, nonché redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il loro controllo

i Nei rapporti tra Allianz Bank e la società di revisione sono adottati i seguenti presidi: (i) massima collaborazione assicurando la completezza e chiarezza delle informazioni fornite, nonché l'accuratezza dei dati e delle elaborazioni; (ii) rispetto della procedura che regolamenta le fasi di valutazione e selezione della società di revisione contabile; (iii) gli incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, vengono conferiti alla società di revisione, previo parere del Collegio Sindacale; (iv) le fasi di selezione della società di revisione contabile e le regole per mantenere l'indipendenza della società di revisione, nel periodo del mandato, aderenti alle disposizioni normative emanate al fine di evitare che l'incarico sia affidato o permanga in capo a società di revisione che si trovano in una situazione di incompatibilità con la Società, sono regolamentate mediante apposite disposizioni aziendali; (v) è vietato il conferimento a soggetti che siano parte della "rete" o del "network" a cui appartiene la società di revisione di incarichi diversi dalla revisione contabile che appaiono incompatibili con quest'ultima, in quanto suscettibili di pregiudicare l'indipendenza della società di revisione incaricata; (vi) l'Assemblea dei Soci viene informata dell'eventuale conferimento di ulteriori incarichi rispetto a quello di revisione contabile alla società di revisione incaricata nonché dell'eventuale conferimento di incarichi a soggetti che siano parte della "rete" o del "network" a cui appartiene la società di revisione;

ii Si dispone inoltre l'attuazione dei seguenti presidi di controllo: (i) attivazione di un programma di formazione e di informazione periodica sulle regole di *corporate governance* e sui reati societari a favore del personale rilevante; (ii) previsione di riunioni periodiche tra il Comitato Consultivo Controlli Interni e Rischi e l'Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di *corporate governance*; (iii) trasmissione al Collegio Sindacale, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge; (iv) attuazione e definizione delle politiche di investimento della Banca attraverso specifici Comitati aziendali all'uopo nominati, operanti in ossequio alla procedura aziendale prevista; (v) formalizzazione e/o aggiornamento di regolamenti interni e procedure aventi ad oggetto l'osservanza della normativa societaria.

- ✓ ***Control Owner*:** Direzione Risorse (per l'erogazione delle attività formative); Unità Organizzativa Segreteria Societaria (per la gestione delle riunioni periodiche e la trasmissione dei documenti relativi all'ordine del giorno): Comitato consultivo Finanza (per la definizione delle politiche di investimento del portafoglio di proprietà della Banca); Comitato Consultivo Rischi (per lo sviluppo, il rispetto e l'eventuale aggiornamento dei Regolamenti interni, le linee guida ed i sistemi di monitoraggio dei limiti)
- ✓ ***Documentazione interna di riferimento***: Procedura Attività di Segreteria Societaria; Procedura Formazione del personale; Allianz Bank Financial Advisors S.p.A. - Progetto di Governo societario e Regolamento Flussi Informativi; Documento di coordinamento del Sistema dei Controlli Interni; Ordine di Servizio Compliance di gruppo 01/2018

e) Gestione delle operazioni di incremento o riduzione del capitale sociale o di altre operazioni su azioni o quote sociali, nonché operazioni di ripartizione degli utili di esercizio, delle riserve e di restituzione dei conferimenti

i Tutte le operazioni sul capitale sociale di Allianz Bank e delle società da essa direttamente controllate nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle regole di *corporate governance* e delle procedure aziendali e di Gruppo e del Gruppo Bancario predisposte

- ✓ ***Control Owner*:** Funzione Risk Management; Segreteria Societaria; Direzione Finanza
- ✓ ***Documentazione interna di riferimento***: Policy in materia di Gestione del Capitale; Procedura Attività di Segreteria Societaria; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Gestione delle operazioni con Soggetti Collegati; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma

f) Approvazione delle delibere consiliari aventi a oggetto operazioni in relazione alle quali gli Amministratori siano portatori di un interesse diverso da quello della Società

i Al momento della loro nomina, ai Consiglieri è richiesto di dichiarare in un apposito *form* l'eventuale partecipazione economica in altre società o presenza di eventuali conflitti di interesse (per se o parti correlate). Successivamente ne è verificata la veridicità attraverso un'interrogazione a sistema da parte della Segreteria Societaria: l'interrogazione a sistema è effettuata ogni qualvolta potrebbe verificarsi la potenziale gestione di un conflitto di interesse.

- ✓ ***Control Owner*:** Unità Organizzativa Compliance e Antiriciclaggio; Unità Organizzativa Segreteria Societaria
- ✓ ***Documentazione interna di riferimento:*** Policy di Gestione dei conflitti di interesse; Procedura Identificazione e gestione dei conflitti di interesse; Politiche in materia di controlli sulle attività di rischio e sui conflitti d'interesse nei confronti di Soggetti Collegati

g) Predisposizione della documentazione che sarà oggetto di discussione e di delibera in Assemblea dei Soci e gestione dei rapporti con tale Organo sociale

i La Banca garantisce la predisposizione, la trasmissione ai Soci e la conservazione della documentazione inerente agli atti e alle deliberazioni dell'Assemblea relative all'approvazione del bilancio, nonché la convocazione e lo svolgimento dell'Assemblea in osservanza dei principi normativi e statutari adottati;

- ✓ ***Control Owner*:** Unità Organizzativa Segreteria Societaria
- ✓ ***Documentazione interna di riferimento***: Procedura Attività di Segreteria Societaria

h) Commercializzazione di prodotti bancari, finanziari e assicurativi, nonché servizi fiduciari

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. l) della Parte Speciale), nonché nel capitolo relativo ai Reati di contraffazione (§4.4, lett. a) della Parte Speciale).

i) Gestione dell'erogazione del credito

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. k) della Parte Speciale).

j) Acquisti di beni, servizi e consulenze

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. g) della Parte Speciale).

k) Partecipazione a gare d'appalto

i La Banca adotta presidi che assicurino trasparenza e tracciabilità dell'intero procedimento di partecipazione alla gara (anche delle fasi gestite dalla "rete") e prevedano la messa a disposizione da parte della funzione competente della necessaria documentazione di supporto;

ii La Banca garantisce che il responsabile del procedimento relazioni con tempestività e compiutezza al responsabile della direzione competente sui singoli avanzamenti del procedimento e comunichi, senza ritardo, al responsabile della direzione competente eventuali comportamenti delle controparti volti ad ottenere favori, elargizioni illecite di denaro o altre utilità anche nei confronti di terzi;

iii La Banca individua preventivamente le funzioni competenti, i criteri e le modalità di partecipazione alle gare e *beauty contest*. La Banca si adopera affinché sia adeguatamente diffusa una politica aziendale improntata a principi di eticità e correttezza nei confronti dei concorrenti in occasione della partecipazione a gare e *beauty contest*;

iv La Banca assicura che il processo di negoziazione, stipula ed esecuzione dei contratti con la Clientela Istituzionale sia tracciabile e prevede l'archiviazione dell'esito dei controlli effettuati nonché di tutta la documentazione inerente al rapporto con il cliente.

- ✓ ***Control Owner*:** Direzione commerciale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione dei rapporti con la Clientela Istituzionale

l) Rapporti con i *media*

i La Banca prevede che i contatti con i *media* vengano intrattenuti per conto della Società unicamente da figure e/o funzioni appositamente e preventivamente individuate

- ✓ ***Control Owner:*** Unità Organizzativa comunicazione esterna
- ✓ ***Documentazione interna di riferimento***: Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma; Procedura Erogazioni liberali; Codice di condotta in materia di regali e intrattenimento; Linee Guida Allianz per l'uso dei social media; Procedura Comunicazione esterna, pubblicitaria e promozionale alla clientela

ii La Banca prevede il divieto di offrire o promettere pagamenti, regali o altri vantaggi, di qualsiasi natura, ad esponenti di organi di informazione, diretti ad influenzarne il giudizio sulla Banca

- ✓ ***Control Owner*:** Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma; Procedura Erogazioni liberali; Codice di condotta in materia di regali e

intrattenimento; Linee Guida Allianz per l'uso dei social media; Procedura Comunicazione esterna, pubblicitaria e promozionale alla clientela

m) Gestione delle controversie e degli accordi transattivi

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5 (m) della Parte Speciale).

n) Gestione degli omaggi, liberalità nonché delle spese di rappresentanza

i La Banca ha adottato – come già si è sottolineato nel capitolo relativo ai Reati nei rapporti con la Pubblica Amministrazione – una specifica *policy* che prevede il divieto di effettuare regali ed inviti, anche a soggetti privati, salvo che rientrino nelle consuete pratiche commerciali; non siano esageratamente generosi, eccessivi o sconvenienti; non possano essere interpretati come una forma di persuasione inappropriata; non influenzino impropriamente il giudizio del destinatario; non violino *policy* e procedure adottate dalla Banca e dal Gruppo (tra cui il Codice Anticorruzione);

- ✓ ***Control Owner*:** Unità organizzativa Compliance e antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Erogazioni liberali; Codice di condotta in materia di regali e intrattenimento; Codice Anticorruzione Gruppo Bancario Allianz Bank

ii La Banca adotta una *policy* che prevede una valutazione collegiale preventiva adeguatamente motivata e documentata in relazione a regali ed inviti che possano potenzialmente presentare criticità ai fini della normativa in esame (sulla base di parametri fissati con apposita *policy* aziendale) e conseguente autorizzazione all'effettuazione dei medesimi solo laddove, a seguito dell'analisi effettuata, vengano ritenute di fatto insussistenti le suddette criticità;

iii Occorre ad ogni modo che i regali o gli omaggi offerti e/o ricevuti siano documentati in modo adeguato e trasparente, in conformità a quanto espressamente previsto dalla procedura di registrazione e approvazione fissata dall'Ordine di servizio in materia di regali e intrattenimento; in caso di dubbio, infine, occorre darne tempestiva informazione alla Funzione *Compliance* di Allianz S.p.A. ai fini di una opportuna valutazione;

- ✓ ***Control Owner*:** Unità organizzativa Compliance e antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Erogazioni liberali; Codice di condotta in materia di regali e intrattenimento; Codice Anticorruzione Gruppo Bancario Allianz Bank

iv La Banca ha inoltre adottato una procedura che prevede una predeterminazione della tipologia di spese rimborsabili; in particolare, il rimborso avviene solo a seguito della presentazione di idonei giustificativi;

- ✓ ***Control Owner*:** Unità Organizzativa Risorse Umane
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle spese di ospitalità e di rappresentanza; Procedura Gestione degli adempimenti amministrativi

v La Banca adotta una *policy* che prevede che l'approvazione del rimborso avvenga da parte di funzione diversa rispetto a quella cui appartiene la persona che richiede il rimborso;

- ✓ ***Control Owner*:** Responsabile della Direzione/Unità Organizzativa per l'autorizzazione della richiesta di rimborso spese; Unità Organizzativa Risorse Umane per l'elaborazione della richiesta di rimborso spese
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle spese di ospitalità e di rappresentanza; Procedura Gestione degli adempimenti amministrativi

o) Selezione, assunzione e gestione del personale

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. h) della Parte Speciale).

p) Selezione dei Consulenti Finanziari abilitati all'offerta fuori sede

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. l) della Parte Speciale).

q) Provvigioni e incentivi ai Consulenti Finanziari abilitati all'offerta fuori sede

i La Banca adotta specifica *policy* aziendale la quale prevede: (i) che le incentivazioni ai consulenti finanziari abilitati all'offerta fuori sede siano riconosciute a fronte di comprovate ragioni che ne giustifichino, a seguito di dettagliata e collegiale valutazione, la dazione; (ii) la tracciatura del processo autorizzativo di concessione delle incentivazioni ai consulenti finanziari abilitati all'offerta fuori sede.

- ✓ ***Control Owner***: Direzione Commerciale; Unità Organizzativa Incentivi (per la definizione degli obiettivi ROR/SII, principali sistemi di incentivazione della Rete dei PFD e dei PFA); Unità Organizzativa Controlli Banca (per la valutazione degli *inducement* identificati come *proper fee*)
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle incentivazioni ai Consulenti finanziari abilitati all'offerta fuori Sede; Procedura Gestione degli incentivi; Policy Gestione degli incentivi; Procedura Gestione del Piano di incentivazione dei Soggetti Rilevanti

ii. La Banca prevede che siano definiti per iscritto anticipatamente e in modo chiaro e trasparente i criteri per maturare il diritto a percepire premi/compensi variabili;

iii. La Banca adotta un sistema di remunerazione che prevede un adeguato equilibrio tra componenti fisse e componenti variabili;

- ✓ ***Control Owner***: Unità Organizzativa Compliance e Antiriciclaggio; Unità Direzione Risorse
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle incentivazioni ai Consulenti finanziari abilitati all'offerta fuori Sede; Procedura Gestione degli incentivi; Policy Gestione degli incentivi; Procedura Gestione del Piano di incentivazione dei Soggetti Rilevanti

r) Gestione di sponsorizzazioni e donazioni

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5(j) della Parte Speciale).

s) Gestione dei servizi di trasporto, custodia e contazione del contante

Si rinvia a quanto previsto nel capitolo relativo ai Reati di contraffazione (§4.4(b) della Parte Speciale).

6. Delitti con finalità di terrorismo

6.1. Le fattispecie di reato rilevanti di cui all'art. 25-*quater*, D.lgs. 231/2001

ASSOCIAZIONI CON FINALITÀ DI TERRORISMO ANCHE INTERNAZIONALE O DI EVERSIONE DELL'ORDINE DEMOCRATICO (ART. 270-*BIS* C.P.)

La condotta punita è quella di chi promuove, costituisce, organizza, dirige, finanzia o partecipa ad associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico.

Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza sono rivolti contro uno Stato estero, un'istituzione e un organismo internazionale.

Esempio

Un Dipendente della Banca accede alla richiesta di apertura di un conto corrente formulata da un esponente di un organismo sospetto di essere coinvolto in attività terroristiche.

FINANZIAMENTO DI CONDOTTE CON FINALITÀ DI TERRORISMO (ART. 270-*QUINQUIES*.1 C.P.)

La condotta punita è quella di chi, al di fuori dei casi di cui agli artt. 270-*bis* c.p. e 270-quater.1 c.p. («*Organizzazione di trasferimenti per finalità di terrorismo*»), raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'art. 270-*sexies* c.p., nonché chiunque deposita o custodisce i beni o il denaro prima indicati.

Esempio

Un Dipendente della Banca accede alla richiesta di apertura di un conto corrente formulata da un soggetto prestanome a beneficio di un soggetto coinvolto in attività terroristiche.

6.2. Processi e attività sensibili rilevanti

In relazione ai Reati con finalità di terrorismo sino a qui descritti, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

- **II.** Gestione dei flussi monetari e finanziari;
- **III.** Selezione e gestione dei Consulenti Finanziari;
- **V.** Commercializzazione dei prodotti bancari, finanziari e assicurativi;
- **VI.** Gestione dell'erogazione del credito;
- **VII.** Acquisto di beni, servizi e consulenze;
- **VIII.** Selezione, assunzione e gestione del personale;
- **IX.** Gestione di omaggi, delle sponsorizzazioni e altre liberalità.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Gestione dell'erogazione del credito;

- Processo Sensibile principale: **VI**

b) Esecuzione di verifiche in fase di rilascio e negoziazione di strumenti di pagamento;

- Processo Sensibile principale: **V**

c) Acquisto di beni, servizi e consulenze;

- Processi Sensibili principali: **II** e **VII**

d) Gestione di sponsorizzazioni e donazioni;

- Processi Sensibili principali: **II** e **IX**

e) Selezione, assunzione e gestione del personale;

- Processo Sensibile principale: **VIII**

f) Selezione dei Consulenti finanziari abilitati all'offerta fuori sede;

- Processo Sensibile principale: **III**

6.3. Principi generali di comportamento

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali, ai Consulenti abilitati all'offerta fuori sede.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*quater* del Decreto e di violare i principi e le procedure aziendali richiamate nella presente Parte Speciale.

Tutti gli obblighi in materia di prevenzione del fenomeno del riciclaggio di denaro previsti dal D.lgs. 231/2007 – che verranno dettagliatamente analizzati nel capitolo 10 della Parte Speciale – devono ritenersi integralmente richiamati anche in questo Capitolo, poiché finalizzati anche alla prevenzione del finanziamento del terrorismo. Si rinvia, quindi, integralmente agli stessi.

Nello svolgimento delle attività aziendali, ad ogni, i Destinatati **devono**:

- assicurare un'approfondita conoscenza dei soggetti con i quali vengono instaurati rapporti nell'esercizio dell'attività bancaria, in particolar modo nelle ipotesi di: instaurazione di un Rapporto Continuativo; esecuzione di operazioni di importo pari o superiore ad Euro 15.000 (sia effettuate con operazione unica o con più operazioni che appaiono collegate o frazionate); acquisizione o modifica di soggetti delegati ad operare sullo stesso rapporto; in sede di chiusura del rapporto continuativo qualora disposta da un soggetto in precedenza non identificato;
- gestire correttamente l'AUI istituito presso la Banca sul quale dovranno essere registrati e conservati i dati identificativi e le altre informazioni relative alle operazioni ed ai rapporti continuativi;
- inviare mensilmente i dati aggregati all'UIF;
- valutare la clientela stessa in funzione del rischio potenziale di commissione dei reati di riciclaggio e di finanziamento del terrorismo; la valutazione del profilo di rischio, da aggiornarsi periodicamente, dovrà basarsi sulla conoscenza della clientela e dovrà tenere conto tanto degli aspetti di carattere oggettivo quanto di carattere soggettivo legati alla stessa, considerando anche le liste di evidenza accentrate e predisponendo controlli rafforzati per determinate categorie di persone;
- segnalare le operazioni sospette all'UIF, anche nel caso in cui le stesse siano rifiutate o comunque non concluse; l'obbligo di effettuare le predette segnalazioni vige per l'intera durata del rapporto con il cliente e non è limitato quindi alle sole fasi d'instaurazione o di chiusura dello stesso (la decisione dei clienti di interrompere un rapporto non rappresenta, di per sé, elemento di sospetto). Le segnalazioni e le comunicazioni devono essere effettuate con la massima tempestività onde consentire all'UIF l'esercizio del potere di sospensione previsto dall'art. 6, comma 6 lett. c), del Decreto Antiriciclaggio.

6.4. Principi specifici per le singole attività sensibili

Con precipuo riferimento alle Attività Sensibili individuate *supra* § 6.2, fermi i divieti generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Gestione dell'erogazione del credito

i La Banca adotta presidi che assicurino un'approfondita conoscenza della clientela al fine di valutare la coerenza e la compatibilità dell'operazione impartita con il profilo del cliente. In particolare, le procedure interne della Banca sono tali da assicurare che il destinatario non figuri nelle liste nominative pubblicate nel sito di Banca d'Italia o risieda in un Paese inserito nelle liste dei Paesi Non Cooperativi (NCCT) pubblicate nel sito del FATF – GAFI. Tali presidi sono: (i) svolgere una istruttoria collegiale tra funzioni diverse al fine di minimizzare il rischio di un'illecita manipolazione di dati; (ii) impartire una adeguata formazione in materia a tutto il personale coinvolto nell'attività di concessione di prestiti bancari; (iii) la tracciabilità scritta di ciascuna fase rilevante nel processo di concessione dei prestiti; (iii) effettuare la rilevazione e l'immediata segnalazione di operazioni ritenute anomale per tipologia, oggetto, frequenza o dimensioni.

ii Agli Organi Sociali ed ai Dipendenti di Allianz Bank (e ai Consulenti Finanziari abilitati all'offerta fuori sede e Consulenti nella misura necessaria alle funzioni dagli stessi svolte) è fatto divieto di: (i) contrattare o, in generale, avere contatti lavorativi con individui inseriti nelle *black list* pubblicate nel sito di Banca d'Italia; (ii) contrattare o, in generale, avere contatti lavorativi con persone fisiche e persone giuridiche residenti o aventi la propria sede in un Paese inserito nelle liste dei Paesi Non Cooperativi (NCCT) pubblicate nel sito del FATF – GAFI; (iii) selezionare personale in azienda i cui requisiti e la cui affidabilità non sia stata adeguatamente esaminata, compatibilmente con la legislazione vigente;

- ✓ ***Control Owner*:** Funzione Antiriciclaggio – Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Perfezionamento contrattuale ed erogazione; Procedura Monitoraggio del credito; Procedura Concessione affidamenti a clienti privati e imprese; Regolamento per la gestione del credito

iii Qualunque erogazione dei fondi deve essere deliberata previa adeguata istruttoria alla quale partecipano soggetti e funzioni diverse all'interno della Banca, in modo da minimizzare il rischio di una manipolazione illecita dei dati ed aumentare la condivisione delle conoscenze e delle decisioni all'interno della Banca;

- ✓ ***Control Owner*:** Unità Organizzativa Crediti; Unità Organizzativa Monitoraggio e Crediti Anomali: Unità Organizzativa Concessioni Nord/Concessioni Sud; Unità Organizzativa Crediti Corporate; Unità Organizzativa Private Credit Specialist; Unità Organizzativa Controlli Rete e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Perfezionamento contrattuale ed erogazione; Procedura Monitoraggio del credito; Procedura Concessione affidamenti a clienti privati e imprese; Regolamento per la gestione del credito

iv L'erogazione del credito da parte di Allianz Bank deve essere eseguita nel rispetto delle regole aziendali previste nel Regolamento per la gestione del credito, predisposto in ottemperanza alle norme di riferimento che regolano gli affidamenti (e in particolare il Testo Unico Bancario) e alle istruzioni di vigilanza per le Banche;

- ✓ ***Control Owner*:** Unità organizzativa crediti
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Perfezionamento contrattuale ed erogazione; Procedura Monitoraggio del credito; Procedura Concessione affidamenti a clienti privati e imprese; Regolamento per la gestione del credito

b) Esecuzione di verifiche in fase di rilascio e negoziazione di strumenti di pagamento

i Le procedure interne della Banca sono tali da assicurare il divieto assoluto di porre strumenti di pagamento a disposizione di soggetti destinatari delle misure di congelamento dei fondi e delle risorse economiche;

ii Le procedure interne della Banca sono tali da assicurare una particolare attenzione ai rapporti con la clientela che comportino flussi di denaro in uscita verso l'estero: in tal senso è necessario verificare che il cliente non risieda in un Paese inserito nelle liste dei Paesi Non Cooperativi (NCCT) pubblicate nel sito del FATF – GAFI e che lo stesso non figuri nelle liste nominative pubblicate nel sito di Banca d'Italia;

iii Le procedure interne della Banca sono tali da assicurare una istruttoria collegiale tra funzioni diverse al fine di minimizzare il rischio di un'illecita manipolazione di dati;

- ✓ ***Control Owner*:** Funzione Antiriciclaggio – Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Controlli Antiriciclaggio; Procedura Gestione e segnalazione frodi sulle carte di pagamento; Procedura Rilascio carnet assegni; Procedura Rilascio e revoca carta di credito

iv Le procedure interne della Banca sono tali da assicurare adeguata formazione in materia a tutto il personale coinvolto nell'attività negoziazione e rilascio di strumenti di pagamento;

- ✓ ***Control Owner***: Responsabile della Funzione antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Controlli Antiriciclaggio; Procedura Gestione e segnalazione frodi sulle carte di pagamento; Procedura Rilascio carnet assegni; Procedura Rilascio e revoca carta di credito

v Le procedure interne della Banca sono tali da assicurare la tracciabilità scritta di ciascuna fase rilevante del processo di negoziazione e rilascio degli strumenti di pagamento;

- ✓ ***Control Owner***: Funzione Antiriciclaggio – Unità Organizzativa Compliance e Antiriciclaggio; Unità Organizzativa Gestione Conto
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Gestione e segnalazione frodi sulle carte di pagamento; Procedura Rilascio carnet assegni; Procedura Rilascio e revoca carta di credito

vi Le procedure interne della Banca sono tali da assicurare la rilevazione e l'immediata segnalazione di operazioni ritenute anomale per tipologia, oggetto, frequenza o dimensioni;

vii La Banca fornisce istruzioni ai Destinatari del Modello affinché gli stessi: (i) non contrattino con soggetti inseriti nelle *black list* pubblicate nel sito di Banca d'Italia e di altri organismi internazionali di prevenzione del terrorismo; (ii) non contrattino con soggetti residenti in un Paese inserito nelle liste dei Paesi Non Cooperativi (NCCT) pubblicate nel sito del FATF – GAFI; (iii) assicurino un'approfondita conoscenza della clientela al fine di valutare la coerenza e la compatibilità delle operazioni impartite con il profilo del cliente; (iv) mantengano aggiornati tutti i dati relativi ai rapporti con i clienti;

- ✓ ***Control Owner***: Funzione Antiriciclaggio – Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Gestione e segnalazione frodi sulle carte di pagamento; Procedura Rilascio carnet assegni; Procedura Rilascio e revoca carta di credito

viii La Banca mantiene costantemente aggiornati tutti i dati relativi ai rapporti con i clienti;

- ✓ ***Control Owner***: Funzione Antiriciclaggio – Unità Organizzativa Compliance e Antiriciclaggio; Unità Organizzativa Anagrafe Clienti; Unità Organizzativa Gestione Conto
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Procedura Gestione anagrafica della clientela; Procedura Rilascio e revoca carta di credito

c) Acquisti di beni, servizi e consulenze

i Agli Organi Sociali ed ai Dipendenti di Allianz Bank (ed ai Consulenti Finanziari abilitati all'offerta fuori sede e Consulenti nella misura necessaria alle funzioni dagli stessi svolte) è fatto divieto di: (i) contrattare o, in generale, avere contatti lavorativi con individui inseriti nelle black list pubblicate nel sito di Banca d'Italia; (ii) contrattare o, in generale, avere contatti lavorativi con persone fisiche e persone giuridiche residenti o aventi la propria sede in un Paese inserito nelle liste dei Paesi Non Cooperativi (NCCT) pubblicate nel sito del FATF – GAFI; (iii) selezionare personale in azienda i cui requisiti e la cui affidabilità non sia stata adeguatamente esaminata, compatibilmente con la legislazione vigente;

- ✓ ***Control Owner***: Funzione Antiriciclaggio – Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Controlli anti frode e anti corruzione; Procedura Manuale Antiriciclaggio; Procedura Organizzativa Controlli Antiriciclaggio

Quanto al processo di selezione di Fornitori e Consulenti, si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. g) della Parte Speciale).

d) Gestione di sponsorizzazioni, donazioni ed erogazione di contributi

i Prima di effettuare una sponsorizzazione o una donazione deve essere verificata la serietà e l'affidabilità del destinatario della stessa attraverso l'accertamento che lo stesso non figuri nelle liste nominative pubblicate nel sito di Banca d'Italia e di altri organismi internazionali di prevenzione del terrorismo o risieda o abbia sede in un Paese inserito nelle liste dei Paesi Non Cooperativi (NCCT) pubblicate nel sito del FATF – GAFI.

- ✓ ***Control Owner***: Unità Organizzativa Controlli Banca; Unità Organizzativa Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Manuale Antiriciclaggio; Codice Anticorruzione Gruppo Bancario Allianz Bank; Procedura Gestione delle sponsorizzazioni della Banca; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma

Quanto all'*iter* decisionale della Banca in relazione a possibili sponsorizzazioni o donazioni, si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. j) della Parte Speciale).

e) Selezione, assunzione e gestione del personale

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5(h) della Parte Speciale).

f) Selezione dei Consulenti Finanziari abilitati all'offerta fuori sede

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5(l) della Parte Speciale).

7. Delitti contro la personalità individuale

7.1. La fattispecie di reato rilevante di cui all'art. 25-*quinquies*, D.lgs. 231/2001

INTERMEDIAZIONE ILLECITA E SFRUTTAMENTO DEL LAVORO (ART. 630-*BIS* C.P.)

Tale reato punisce, salvo che il fatto costituisca un reato più grave, chiunque (1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori; (2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero (1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

Costituiscono, in particolare, indice di sfruttamento la sussistenza di una o più delle seguenti condizioni (**i**) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato; (**ii**) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie; (**iii**) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro; (**iv**) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Esempio

La Banca, a seguito di una revisione in aumento delle retribuzioni dei Dipendenti previste dal CCNL applicato, decide di licenziare una serie di Lavoratori e affidare tali attività a un ente che recluta manodopera facendola lavorare in condizione di sfruttamento approfittando dello stato di bisogno dei lavoratori.

7.2. Processi e attività sensibili rilevanti

In relazione al reato di intermediazione illecita e sfruttamento del lavoro descritto, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

VII. Acquisto di beni, servizi e consulenze;

VIII. Selezione, assunzione e gestione del personale.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Gestione del personale, con particolare riferimento alla definizione dell'orario di lavoro, delle condizioni retributive e del rispetto della normativa a tutela della salute e sicurezza sui luoghi di lavoro

- Processo Sensibile principale: **VIII**

b) Gestione degli acquisti, con particolare riferimento all'affidamento di attività che prevedano l'utilizzo di manodopera di terze parti per la fornitura di personale e/o servizi (p.e., appalti di opere e di servizi)

- Processo Sensibile principale: **VII**

7.3. Principi generali di comportamento

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali ai Consulenti Finanziari abilitati all'offerta fuori sede.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*quinquies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

A tal fine, la Banca (**i**) considera *sempre* prevalente la tutela dei diritti delle persone e dei lavoratori rispetto a qualsiasi considerazione di carattere economico; (**ii**) assicura massima tracciabilità e trasparenza nella gestione dei rapporti con società che svolgono attività in appalto per conto di Allianz Bank; (**iii**) si attiene alle condizioni normative e retributive non inferiori a quelle risultanti dai CCNL applicabili; (**iv**) assicura regolarità nei pagamenti e negli adempimenti previdenziali, assistenziali e assicurativi, nonché in tutti gli altri obblighi previsti dalla normativa di riferimento.

7.4. Principi specifici per le singole attività sensibili

Con riferimento alle Attività Sensibili individuate *supra* § 7.2, fermi i principi generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Gestione del personale, con particolare riferimento alla definizione: dell'orario di lavoro, delle condizioni retributive e del rispetto della normativa a tutela della salute e sicurezza sui luoghi di lavoro

i La Banca si impegna ad ottemperare a tutti gli obblighi verso i Dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro ed assicurazioni sociali, assumendo a suo carico tutti gli oneri relativi;

ii La Banca si obbliga, ad applicare, nei confronti dei propri Dipendenti, condizioni normative e retributive non inferiori a quelle risultanti dai CCNL applicabili alla categoria e nella località in cui si svolgono le prestazioni, nonché le condizioni risultanti da successive modifiche o integrazioni;

- ✓ ***Control Owner*:** Unità Organizzativa Risorse Umane; Unità Organizzativa Amministrazione e Gestione del Personale
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e valutazione del personale e politiche retributive; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma

iii La Banca si obbliga a continuare ad applicare i suindicati CCNL anche dopo la loro scadenza e fino alla loro sostituzione;

- ✓ ***Control Owner*:** Unità Organizzativa Risorse Umane; Unità Organizzativa Amministrazione e Gestione del Personale
- ✓ ***Documentazione interna di riferimento***: Procedura Selezione e valutazione del personale e politiche retributive

iv La Banca assicura che, qualora l'adempimento delle attività descritte ai punti precedenti avvenisse ricorrendo ai servizi di un'agenzia esterna specializzata, il rapporto con quest'ultima sia disciplinato da accordo scritto, il quale preveda l'obbligo dell'agenzia esterna a non porre in essere comportamenti che violino le disposizioni di cui al Decreto e a rispettare per quanto applicabile il Modello della Banca;

- ✓ ***Control Owner*:** Unità Organizzativa Consulenza Legale Banca; Responsabile Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

b) Gestione degli acquisti, con particolare riferimento all'affidamento di attività che prevedano l'utilizzo di manodopera di terze parti per la fornitura di personale e/o servizi (p.e., appalti di opere e di servizi)

i La Banca si assicura che nei contratti di appalto sia inserito l'impegno da parte dell'appaltatore a ottemperare a tutti gli obblighi verso i dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro ed assicurazioni sociali, assumendo a suo carico tutti gli oneri relativi;

ii La Banca si assicura che nei contratti di appalto sia inserito l'obbligo da parte dell'appaltatore di applicare, nei confronti dei propri dipendenti, condizioni normative e retributive non inferiori a quelle risultanti dai CCNL applicabili alla categoria e nella località in cui si svolgono le prestazioni, nonché le condizioni risultanti da successive modifiche o integrazioni;

iii La Banca si assicura che nei contratti di appalto sia inserito l'obbligo da parte dell'appaltatore di continuare ad applicare i suindicati CCNL anche dopo la loro scadenza e fino alla loro sostituzione;

iv La Banca si assicura che nei contratti di appalto sia inserito l'impegno da parte dell'appaltatore di fornire all'atto della sottoscrizione del contratto e successivamente con periodicità stabilita dalle parti (per esempio, ogni tre mesi) copia del documento unico di regolarità contributiva (c.d. DURC) relativo alla posizione amministrativa dell'appaltatore e dei propri subappaltatori rilasciato dalle competenti autorità;

v La Banca si assicura che nei contratti di appalto sia inserita la facoltà da parte della Società di richiedere in ogni momento copia del libro unico del lavoro (c.d. LUL) tenuto dall'appaltatore e da eventuali subappaltatori;

vi La Banca si assicura che nei contratti di appalto sia inserito l'obbligo dell'appaltatore a non porre in essere comportamenti che violino le disposizioni di cui al Decreto e a rispettare per quanto applicabile il Modello della Società;

vii La Banca si assicura che nei contratti di appalto sia inserito l'impegno da parte della Società a regolare tutti i rapporti con i propri appaltatori ed eventuali subappaltatori mediante accordi contrattuali che prevedano il rispetto dei principi del presente capitolo di Parte Speciale sui reati contro la personalità individuale;

viii La Banca si assicura che nei contratti di appalto sia prevista la possibilità di verificare attraverso controlli, anche in loco, il rispetto delle condizioni di cui ai contratti che regolano i rapporti sopracitati;

ix La Banca si assicura che nei contratti di appalto sia inserita la facoltà da parte della Società di richiedere in ogni momento tutta la documentazione utile a verificare l'origine, le condizioni e il trattamento della forza lavoro;

x La Banca si assicura che nei contratti di appalto sia inserita la facoltà da parte della Società, qualora siano in qualsiasi modo accertate eventuali violazioni delle disposizioni sull'intermediazione e sullo sfruttamento del lavoro, di risolvere il contratto con l'appaltatore.

- ✓ ***Control Owner*:** Unità Organizzativa Consulenza Legale Banca; Responsabile Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

8. Abusi di mercato

8.1. Le fattispecie di reato rilevanti di cui all'art. 25-*sexies*, D.lgs. 231/2001 e gli illeciti amministrativi di cui al D.lgs. 58/1998

Per contrastare i fatti di *market abuse*, il legislatore italiano ha deciso di affiancare alle sanzioni penali di cui agli artt. 184 e 185 del D.lgs. 58/1998 anche dei presidi di carattere amministrativo contemplati dagli artt. 187-*bis* e 187-*ter* del D.lgs. 58/1998. Come per le persone fisiche, un sistema sanzionatorio a c.d. *doppio binario* è stato previsto anche per le persone giuridiche: infatti, insieme all'art. 25-*sexies* del Decreto – che richiama gli artt. 184 e 185 D.lgs. 58/1998 – nel nostro ordinamento è inoltre prevista anche un'ipotesi di responsabilità amministrativa dell'ente "da illecito amministrativo". Tale responsabilità amministrativa "diretta" dell'ente è, in particolare, contemplata dall'art. 187-*quinquies* D.lgs. 58/1998, e configurata alla stregua di una conseguenza della commissione degli illeciti amministrativi di abuso di mercato (artt. 187-*bis* e 187-*ter* D.lgs. 58/1998), nell'interesse o a vantaggio dell'ente, da parte di soggetti 'apicali' o subordinati. L'art. 187-*quinquies*, inoltre, prevede l'esonero da responsabilità dell'ente che provi che gli autori dell'illecito amministrativo abbiano agito esclusivamente nell'interesse proprio o di terzi e richiama, in quanto compatibili, gli articoli 6, 7, 8 e 12 del D.lgs.n.231/2001.

Per tale ragione, insieme alla descrizione delle due ipotesi di reato, in questo paragrafo si fornirà una descrizione anche dei due illeciti amministrativi. Come anticipato nel capitolo relativo ai Reati societari, per affinità di materia, si riporta in questa sede anche la fattispecie di cui all'art. 2637 c.c. («*Aggiotaggio*»).

ABUSO DI INFORMAZIONI PRIVILEGIATE (ART. 184 D.LGS. 58/1998)

A seguito delle modifiche apportate dal D.lgs. 107/2018, recante «*Norme di adeguamento della normativa nazionale al regolamento (UE) n. 596/2014*» (c.d. *Market Abuse Regulation* o MAR), il reato di abuso di informazioni privilegiate punisce «*chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale azionario dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, 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; (b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014; c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera (a)*» (art. 184, co. 1, D.lgs. 58/1998).

Per «*strumenti finanziari*», l'articolo appena riportato intende quelli negoziati (o per i quali è stata presentata richiesta di ammissione alla negoziazione) in un mercato regolamentato.

Il medesimo articolo sanziona poi con una contravvenzione le stesse condotte nel caso di operazioni relative a strumenti finanziari negoziati (o per i quali è stata presentata richiesta alla negoziazione) su sistemi multilaterali di negoziazione, su sistemi organizzati di negoziazione, ovvero in relazione a strumenti finanziari il cui prezzo o valore dipende dal prezzo o valore o ha un effetto sul prezzo o valore di uno strumento finanziario negoziato su un sistema multilaterale di negoziazione o su un sistema organizzato di negoziazione, nonché di operazioni relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote o di emissioni.

A seguito del D.lgs. 107/2018, inoltre, la definizione di «*informazione privilegiata*» rilevante è quella di cui all'art. 7 del MAR. In particolare, per informazione privilegiata 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 essa fa riferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà e se tale informazione è sufficientemente specifica da permettere di

trarre conclusioni sul possibile effetto di detto complesso di circostanze o di detto evento 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 emissioni. A tal riguardo, nel caso di un processo prolungato che è inteso a concretizzare, o che determina, una particolare circostanza o un particolare evento, tale futura circostanza o futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della circostanza o dell'evento futuri, possono essere considerate come informazioni aventi carattere preciso.

Una *tappa intermedia* in un processo prolungato è considerata un'informazione privilegiata se risponde ai criteri fissati nel presente articolo riguardo alle informazioni privilegiate.

Per informazione che, se comunicata al pubblico, avrebbe probabilmente un *effetto significativo sui prezzi degli strumenti finanziari*, degli strumenti finanziari derivati, dei contratti a pronti su merci collegati o dei prodotti oggetto d'asta sulla base di quote di emissioni, s'intende un'informazione che un investitore ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni di investimento.

ABUSO E COMUNICAZIONE ILLECITA DI INFORMAZIONI PRIVILEGIATE (ART. 187-*BIS* D.LGS. 58/1998)

Quanto all'illecito amministrativo di abuso di informazioni privilegiate, con il D.lgs. 107/2018 il legislatore italiano ha optato per un rinvio secco alle disposizioni contenute nel MAR. L'art. 187-bis del D.lgs. 58/1998, infatti, ora punisce «*chiunque viola il divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate di cui all'articolo 14 del regolamento (UE) n. 596/2014*».

Rilevanti ai sensi dell'art. 14 MAR, in particolare, le fattispecie descritte dall'art. 8 e dall'art. 10 del medesimo regolamento.

Nello specifico, ai sensi dell'art. 8, par. 1, MAR «*si ha abuso di informazioni privilegiate quando una persona in possesso di informazioni privilegiate utilizza tali informazioni acquisendo o cedendo, per conto proprio o per conto terzi, direttamente o indirettamente, gli strumenti finanziari cui tali informazioni si riferiscono*». È inoltre considerato abuso di informazioni privilegiate «*l'uso di dette informazioni tramite l'annullamento o modifica di un ordine concernente uno strumento finanziario al quale le informazioni si riferiscono quando tale ordine è stato inoltrato prima che la persona interessata entrasse in possesso di dette informazioni privilegiate*». Inoltre, in relazione alle aste di quote di emissione (o di altri prodotto correlati) «*l'uso di informazioni privilegiate si configura anche quando una persona presenta, modifica o ritira un'offerta per conto proprio o per conto di terzi*».

Inoltre, ai sensi dell'art. 8, par. 2, MAR «*si ha raccomandazione che un'altra persona compia abusi di informazioni privilegiate o induzione di un'altra persona a compiere abusi di informazioni privilegiate quando la persona è in possesso di informazioni privilegiate e: (a) raccomanda, sulla base di tali informazioni, che un'altra persona acquisisca o ceda strumenti finanziari a cui tali informazioni si riferiscono o induce tale persona a effettuare l'acquisizione o la cessione; ovvero (b) raccomanda, sulla base di tali informazioni, a un'altra persona di cancellare o modificare un ordine concernente uno strumento finanziario cui si riferiscono le informazioni o induce tale persona a effettuare la cancellazione o la modifica*».

L'illecito amministrativo punisce indistintamente gli insider c.d. *primari* – i.e., chi possiede informazioni privilegiate perché membro di organi amministrativi, di direzione o di controllo dell'emittente o partecipante al mercato delle quote di emissione; chi detiene una partecipazione al capitale dell'emittente o di un partecipante al mercato delle quote di emissione; chi ha accesso a tali informazioni nell'esercizio di un'occupazione, di una professione o di una funzione; chi è coinvolto in attività criminali – e i gli insider c.d. *secondari*. In particolare, per insider secondari si intende qualsiasi persona che detiene informazioni privilegiate per circostanze diverse rispetto a quelle elencate per gli insider primari «quando detta persona sa o dovrebbe sapere che si tratta di informazioni privilegiate» (art. 8, par. 4, co. 2, MAR).

In relazione alla condotta di raccomandazione e induzione, viene punita anche la persona che riceve (e usa) le stesse quando «*sa o dovrebbe sapere che esse si basano su informazioni privilegiate*» (art. 8, par. 3, MAR).

Il *Market Abuse Regulation* ha poi scorporato dalla condotta di abuso di informazioni privilegiate quella di comunicazione illecita di informazioni privilegiate (c.d. *tipping*). È infatti l'art. 10 del MAR a descrivere questo illecito: nello specifico, si ha «*comunicazione illecita di informazioni privilegiate quando una persona è in possesso di informazioni privilegiate e comunica tali informazioni a un'altra persona, tranne quando la comunicazione avviene durante il normale esercizio di un'occupazione, una professione o una funzione*». Anche questo articolo si applica a tutti gli insider primari sopra menzionati e agli insider secondari.

Anche in questo caso, viene ora punita anche la condotta di chi comunica non solo informazioni privilegiate ma anche raccomandazioni o induzioni a commettere abuso di informazioni privilegiate quando «*la persona che comunica la raccomandazione o l'induzione sa o dovrebbe sapere che esse si basano su informazioni privilegiate*» (art. 10, par. 2, MAR).

Esempi

Un Dipendente di Allianz Bank nell'esame della posizione di un emittente quotato, potenziale cliente, viene in possesso di informazioni privilegiate che utilizza per compiere operazioni sul mercato.

Un Dipendente di Allianz Bank nell'esame della posizione di un emittente quotato, potenziale cliente, viene in possesso di informazioni privilegiate e, sulla base di esse, raccomanda operazioni sul mercato a un soggetto terzo.

Un Dipendente di Allianz Bank nell'esame della posizione di un emittente quotato, potenziale cliente, viene in possesso di informazioni privilegiate e le comunica al di fuori del normale esercizio del proprio ufficio (es. le racconta a un amico o anche a un collega non coinvolto nel progetto).

AGGIOTAGGIO (ART. 2637 C.C.)

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

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

Esempio

L'Amministratore Delegato della Banca diffonde al mercato una falsa notizia idonea ad incidere in modo significativo sull'affidamento che il pubblico ripone sulla stabilità patrimoniale del Gruppo Bancario.

MANIPOLAZIONE DEL MERCATO (ART. 185 D.LGS. 58/1998)

L'illecito penale di manipolazione del mercato – che, a differenza dell'ipotesi di aggiotaggio di cui al codice civile – riguarda strumenti finanziari quotati (o per i quali è stata richiesta ammissione alla negoziazione), è disciplinato dall'art. 185 del D.lgs. 58/1998 che punisce «*chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumento finanziari*».

Come per l'abuso di informazioni privilegiate, anche l'art. 185 prevede un'ipotesi contravvenzionale qualora le medesime condotte riguardino strumenti finanziari negoziati su sistemi multilaterali di negoziazione, su sistemi organizzati di negoziazione, ovvero strumenti finanziari il cui prezzo o valore dipende dal prezzo o valore o ha un effetto sul prezzo o valore di uno strumento finanziario negoziato su un sistema multilaterale di negoziazione o su un sistema organizzato di negoziazione, nonché operazioni relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote o di emissioni.

Inoltre, a seguito del D.lgs. 107/2018, l'ambito di applicazione dell'articolo 185 del D.lgs. 58/1998 è stato ulteriormente esteso «*ai fatti concernenti gli strumenti finanziari, compresi i contratti derivati per il trasferimento del rischio del credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronto*

su merci, qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari», nonché «ai fatti concernenti gli indici di riferimento (benchmark)» (art. 185, co. 2-*ter*, D.lgs. 58/1998).

MANIPOLAZIONE DEL MERCATO (ART. 187-*TER* D.LGS. 58/1998)

A seguito dell'opera di adeguamento alle disposizioni del *Market Abuse Regulation*, anche l'art. 187-*ter* del D.lgs. 58/1998, relativo all'illecito amministrativo di manipolazione del mercato, rinvia ora direttamente alle disposizioni del regolamento sugli abusi di mercato. Ai sensi del medesimo articolo, infatti, è punito «*chiunque viola il divieto di manipolazione del mercato di cui all'articolo 15 del regolamento (UE) n 596/2014*».

Nello specifico, il divieto di cui all'art. 15 MAR si riferisce alle condotte descritte dall'art. 12, par. 1 del medesimo regolamento, ai sensi del quale si intendono per manipolazione del mercato le seguenti attività: (**a**) l'avvio di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra condotta che: (i) invii, o è probabile che invii, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni; oppure (ii) consenta, o è probabile che consenta, di fissare il prezzo di mercato di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale o artificiale; (**b**) a meno che la persona che avvia un'operazione, inoltra un ordine di compravendita o ha posto in essere qualsiasi altra condotta stabilisca che tale operazione, ordine o condotta sono giustificati da legittimi motivi e sono conformi a una pratica di mercato ammessa, l'avvio di un'operazione, l'inoltro di un ordine di compravendita o qualsiasi altra attività o condotta che incida, o sia probabile che incida, sul prezzo di uno o più strumenti finanziari, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni, utilizzando artifici o qualsiasi altra forma di raggiro o espediente; (**c**) la diffusione di informazioni tramite i mezzi di informazione, compreso Internet, o tramite ogni altro mezzo, che forniscano, o siano idonei a fornire, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di uno strumento finanziario, di un contratto a pronti su merci collegato o di un prodotto oggetto d'asta sulla base di quote di emissioni o che consentano, o è probabile che consentano, di fissare il prezzo di mercato di uno o più strumenti finanziari o di contratti a pronti su merci collegati o di un prodotto oggetto d'asta sulla base di quote di emissioni a un livello anormale o artificiale, compresa la diffusione di voci, quando la persona che ha proceduto alla diffusione sapeva, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti; (**d**) la trasmissione di informazioni false o fuorvianti o la comunicazione di dati falsi o fuorvianti in relazione a un indice di riferimento (c.d. *benchmark*) quando la persona che ha proceduto alla trasmissione o fornito i dati sapeva, o avrebbe dovuto sapere, che erano falsi o fuorvianti, ovvero qualsiasi altra condotta che manipola il calcolo di un indice di riferimento.

L'art. 12, par. 2 del MAR, a sua volta, fornisce delle esemplificazioni di condotte che, tra le altre, devono essere considerate manipolazione del mercato.

Esempio

Un Dipendente, al di fuori della normativa e delle regole e procedure interne, rilascia al pubblico una notizia errata riguardo a una imminente e importante operazione relativa a strumenti finanziari quotati che Allianz Bank si appresta a concludere; la diffusione della notizia è idonea ad incidere sensibilmente sul prezzo degli strumenti finanziari, a vantaggio della Banca.

8.2. Processi e attività sensibili rilevanti

In relazione ai reati e agli illeciti amministrativi sin qui descritti, i Processi Sensibili della Banca potenzialmente più esposti al rischio sono i seguenti:

- **XII.** Gestione dei rapporti con i *media* e delle informazioni privilegiate;
- **XV.** Gestione degli investimenti.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Comunicazioni all'esterno (*e.g.*, CONSOB, Banca d'Italia, analisti finanziari, azionisti, giornalisti, ecc.)

- Processo Sensibile principale: **XII**

b) Gestione delle informazioni privilegiate relative ad Allianz SE ed in genere a tutte le società quotate

- Processo Sensibile principale: **XII**

c) Identificazione delle operazioni sospette ai sensi del Regolamento CONSOB recante norme di attuazione del Decreto Legislativo 24 febbraio 1998, n. 58 in materia di mercati

- Processo Sensibile principale: **XII**

d) Operazioni personali aventi ad oggetto strumenti finanziari

- Processo Sensibile principale: **XII** e **XV**

8.3. Principi generali di comportamento

I divieti generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*quinquies* del Decreto, agli illeciti amministrativi di cui agli artt. 187-*bis* e 187-*ter* D.lgs. 58/1998, il reato di aggiotaggio di cui all'art. 2637 c.c. e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

In particolare, in relazione all'attività di **trattamento di informazioni privilegiate**, ai Destinatari è fatto **divieto** di:

- utilizzare informazioni privilegiate relative a strumenti finanziari o emittenti strumenti finanziari quotati, comunque ottenute, per negoziare, direttamente o indirettamente, strumenti finanziari, sia per conto e/o nell'interesse della Banca, sia in nome e per conto proprio o di terzi;
- partecipare su internet a gruppi di discussione o *chatroom* aventi ad oggetto strumenti finanziari o emittenti strumenti finanziari, quotati o non quotati, e nei quali vi sia uno scambio di informazioni concernenti il Gruppo Allianz, le sue società, le società concorrenti o le società quotate in genere o gli strumenti finanziari emessi da tali soggetti, a meno che non si tratti di incontri istituzionali per i quali è già stata compiuta una verifica di legittimità da parte delle funzioni competenti o non vi sia scambio di informazioni il cui carattere non privilegiato sia evidente;
- sollecitare l'ottenimento di Informazioni Privilegiate su strumenti finanziari o emittenti strumenti finanziari quotati, se non in base ad accordi contrattuali o ai sensi della normativa applicabile.

In particolare, in relazione alle attività di **diffusione di informazioni o valutazioni**, ai Destinatari è fatto **divieto** di:

- effettuare comunicazioni istituzionali senza il preventivo coordinamento con le funzioni preposte a tale compito e senza rispettare le procedure in materia;
- rivelare a terzi informazioni privilegiate relative al Gruppo Allianz o relative a strumenti finanziari o emittenti strumenti finanziari quotati, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità;
- comunicare o diffondere all'esterno analisi o valutazioni su uno strumento finanziario quotato (o sul suo emittente), che possano influenzare i terzi, dopo aver precedentemente preso posizione sullo strumento finanziario, beneficiando di conseguenza dell'impatto della valutazione diffusa sul prezzo di detto

strumento, senza avere allo stesso tempo comunicato al pubblico, in modo corretto ed efficace, l'esistenza di tale conflitto di interesse;

- diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo;
- tenere altri comportamenti preordinati alla diffusione di informazioni false o fuorvianti, anche tramite canali diversi dai mezzi di comunicazione di massa;
- diffondere al pubblico valutazioni o notizie su uno strumento finanziario o un emittente senza prima aver verificato, per il tramite di fonti istituzionali autorizzate, l'attendibilità della fonte ed essersi accertati circa il carattere non privilegiato dell'informazione;
- comunicare a chiunque le informazioni riguardanti il *management* della Banca, anche quando riguardi la posizione personale del soggetto agente, se non dopo la comunicazione ufficiale della Banca;
- raccomandare o indurre terzi ad effettuare operazioni su strumenti finanziari sulla base di informazioni privilegiate comunque ottenute;
- in generale, comunicare a terzi, al di fuori del normale e legittimo esercizio del proprio lavoro, Informazioni Privilegiate in qualsiasi modo ottenute.

Ancora, nell'ambito delle **attività di investimento** della Banca, è fatto esplicitamente **divieto** a tutti i Destinatari di:

- agire di concerto o consultandosi con altri soggetti per acquisire una posizione dominante sull'offerta o sulla domanda di uno strumento finanziario che abbia l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette;
- acquistare o vendere strumenti finanziari alla chiusura del mercato con l'effetto di ingannare gli investitori che operano sulla base dei prezzi di chiusura;
- effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle forme previste dalla normativa e dalle procedure aziendali) e se tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;
- effettuare operazioni di acquisto o di vendita di uno strumento finanziario senza che si determini alcuna variazione negli interessi o nei diritti o nei rischi di mercato del beneficiario delle operazioni o dei beneficiari che agiscono di concerto o in modo collusivo (le operazioni di riporto o di prestito titoli o le altre operazioni che prevedono il trasferimento di strumenti finanziari in garanzia non costituiscono di per sé manipolazione del mercato);
- inserire ordini a prezzi più alti (bassi) di quelli delle proposte presenti dal lato degli acquisti (vendite) al fine di fornire indicazioni fuorvianti dell'esistenza di una domanda (offerta) sullo strumento finanziario a tali prezzi più elevati (bassi);
- acquistare o vendere intenzionalmente strumenti finanziari o contratti derivati verso la fine delle negoziazioni in modo da alterare il prezzo finale dello strumento finanziario o del contratto derivato;
- agire di concerto con altri operatori sul mercato secondario, dopo un collocamento effettuato nell'ambito di un'offerta al pubblico, al fine di mantenere il prezzo di uno strumento finanziario quotato verso livelli artificiali;
- abusare della propria posizione dominante in modo da distorcere significativamente il prezzo al quale altri operatori sono obbligati, per l'assolvimento dei loro impegni, a consegnare o ricevere o rinviare la consegna dello strumento finanziario o del prodotto sottostante;
- concludere operazioni o impartire ordini in modo tale da evitare che i prezzi di mercato degli strumenti finanziari del Gruppo scendano al disotto di un certo livello, principalmente per sottrarsi alle conseguenze

negative derivanti dal connesso peggioramento del rating degli strumenti finanziari emessi. Questo comportamento deve essere tenuto distinto dalla conclusione di operazioni rientranti nei programmi di acquisto di azioni proprie o nella stabilizzazione degli strumenti finanziari previsti dalla normativa;

- concludere operazioni in un mercato su uno strumento finanziario con la finalità di influenzare impropriamente il prezzo dello stesso strumento finanziario o di altri strumenti finanziari collegati negoziati sullo stesso o su altri mercati (ad esempio, concludere operazioni su azioni per fissare il prezzo del relativo strumento finanziario derivato negoziato su un altro mercato a livelli anomali, oppure effettuare operazioni sul prodotto sottostante a uno strumento finanziario derivato per alterare il prezzo dei relativi contratti derivati. Le operazioni di arbitraggio non costituiscono di per sé manipolazione del mercato);
- concludere un'operazione o una serie di operazioni per nascondere quale sia la vera proprietà di uno strumento finanziario, tramite la comunicazione al pubblico - in violazione alle norme che regolano la trasparenza degli assetti proprietari - della proprietà di strumenti finanziari a nome di altri soggetti collusi (questo comportamento non riguarda i casi in cui esistono motivi legittimi che consentono l'intestazione degli strumenti finanziari in nome di un soggetto diverso dal proprietario. Inoltre, una scorretta comunicazione di una partecipazione rilevante non implica necessariamente una manipolazione del mercato);
- aprire una posizione lunga su uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere fuorvianti informazioni positive sullo strumento finanziario in modo da aumentarne il prezzo;
- prendere una posizione ribassista su uno strumento finanziario ed effettuare un'ulteriore attività di vendita e/o diffondere fuorvianti informazioni negative sullo strumento finanziario in modo da ridurne il prezzo;
- aprire una posizione su uno strumento finanziario e chiuderla immediatamente dopo che la posizione stessa è stata resa nota al pubblico;
- operare creando inusuali concentrazioni di operazioni in concerto con altri soggetti su un particolare strumento finanziario;
- vendere la totalità o la quasi totalità degli strumenti finanziari presenti nel portafoglio per investire la liquidità ricavata su uno specifico strumento finanziario, a meno che tale operazione non risulti specificamente approvata dai competenti organi aziendali e sulla base delle deleghe interne conferite;
- richiedere l'immediata esecuzione di un ordine senza indicazioni di prezzo;
- realizzare un'inusuale operatività sugli strumenti finanziari di una società emittente prima dell'annuncio di informazioni privilegiate relative alla società, a meno che tale operatività non sia basata su analisi di mercato, su informazioni non privilegiate ovvero su altre notizie pubblicamente disponibili;
- realizzare operazioni senza alcuna altra motivazione che quella di aumentare o ridurre il prezzo di uno strumento finanziario o di aumentare i quantitativi scambiati su uno strumento finanziario;
- realizzare operazioni che hanno la finalità di aumentare il prezzo di uno strumento finanziario nei giorni precedenti all'emissione di uno strumento finanziario derivato collegato o di uno strumento finanziario convertibile;
- realizzare operazioni che, proprio nei giorni precedenti l'emissione di uno strumento finanziario derivato collegato o di uno strumento finanziario convertibile, hanno la finalità di sostenere il prezzo dello strumento finanziario in presenza di un andamento discendente dei prezzi di tale strumento finanziario;
- realizzare operazioni che hanno la finalità di modificare la valutazione di una posizione senza che venga modificata, in aumento o in diminuzione, la dimensione della posizione stessa;

- effettuare operazioni che nel giorno di scadenza di uno strumento finanziario derivato hanno la finalità di mantenere il prezzo dello strumento finanziario sottostante al disotto del prezzo di esercizio dello strumento finanziario derivato;
- effettuare operazioni che nel giorno di scadenza di uno strumento finanziario derivato sono finalizzate a far passare il prezzo dello strumento finanziario sottostante al disopra del prezzo di esercizio dello strumento finanziario derivato;
- omettere di comunicare le operazioni sospette individuate secondo le specifiche procedure predisposte in materia alla funzione preposta alla raccolta delle segnalazioni stesse. Tale divieto è operativo anche con riferimento alla prestazione del servizio di ricezione e trasmissione di ordini;
- porre in essere o tentare di porre in essere operazioni od ordini di compravendite che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- compiere operazioni su strumenti finanziari dopo essere venuti a conoscenza di informazioni privilegiate riguardanti strumenti finanziari, anche qualora tali operazioni siano state decise in precedenza attraverso un autonomo processo di scelta di investimento. Nei casi dubbi potrà essere chiesto il parere della funzione Compliance della Banca e/o della Funzione *Compliance* di Allianz S.p.A.

8.4. Principi specifici per le singole attività sensibili

Con riferimento alle Attività Sensibili individuate *supra* § 8.2, fermi i principi generali di comportamento appena richiamati, si applicano i seguenti principi specifici.

a) Comunicazioni all'esterno (*e.g.,* CONSOB, IVASS, analisti finanziari, azionisti, giornalisti, ecc.), e

b) Gestione delle informazioni privilegiate relative ad Allianz SE ed in genere a tutte le società quotate

i Il trattamento delle informazioni privilegiate deve avvenire nel rispetto delle relative disposizioni organizzative interne in cui sono indicati compiti e i ruoli dei soggetti responsabili della gestione di tali informazioni, le norme che regolano la diffusione delle medesime e le modalità che i responsabili sono tenuti ad utilizzare per il loro trattamento e la loro pubblicazione. In ogni caso ogni qualvolta sussista il dubbio se un'informazione rivesta il carattere di informazione privilegiata prima di essere diffusa o trasmessa dovrà essere richiesto il parere preventivo della funzione responsabile come indicata nelle procedure aziendali;

- ✓ ***Control Owner*:** Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Market Abuse: gestione delle operazioni sospette; Procedura Identificazione e gestione delle operazioni personali; Regolamento per il contrasto al Market Abuse

ii La Banca predispone, all'interno del piano formativo per i Dipendenti, un programma di formazione-informazione periodica sui reati e gli illeciti amministrativi di *market abuse* e sulle relative procedure aziendali in essere;

- ✓ ***Control Owner*:** Responsabile di Unità Organizzativa – Unità Organizzativa Formazione, selezione e relazioni sindacali
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle Risorse umane – Formazione del personale

iii I responsabili deputati alla gestione delle informazioni privilegiate istituiscono un registro delle persone in possesso delle informazioni privilegiate secondo quanto previsto dall'art. 115-*bis* del D.lgs. 58/1998;

- ✓ ***Control Owner*:** Direzione Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Identificazione e gestione delle operazioni personali

iv La Funzione *Compliance* di Allianz S.p.A. richiede ai soggetti iscritti nelle *Insider List* di fornire le evidenze della movimentazione di eventuali depositi titoli per cui gli stessi risultano intestatari/cointestatari/con delega ad operare;

- ✓ ***Control Owner*:** Funzione Compliance di Gruppo
- ✓ ***Documentazione interna di riferimento***: Codice Etico e di Comportamento; Allianz Standard for Capital Markets Compliance; Procedura Capital Markets - Insider List e gestione delle operazioni personali; Regolamento per il contrasto al Market Abuse

c) Identificazione delle operazioni sospette ai sensi del Regolamento CONSOB recante norme di attuazione del decreto legislativo 24 febbraio 1998, n. 58 in materia di mercati

i La Banca adotta una procedura volta a definire: (i) ruoli e responsabilità di ciascuna delle strutture e dei soggetti della Banca coinvolti nel processo di rilevazione, gestione e segnalazione delle operazioni sospette ai sensi della normativa in ambito di *market abuse;* (ii) il modello operativo adottato dalla Banca per lo svolgimento delle attività di analisi relative alle segnalazioni delle operazioni sospette;

- ✓ ***Control Owner*:** Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Regolamento per il contrasto del Market Abuse

ii Ciascun Dipendente o collaboratore o personale di contatto della Banca, nel caso in cui nutra il ragionevole sospetto in ordine ad una o più operazioni effettuata/e dalla Banca sia per conto della clientela che per conto proprio del portafoglio di proprietà, a prescindere dalla sussistenza dei presupposti oggettivi (indicatori di anomalia), è tenuto a compilare un'apposita scheda adottata dalla Banca («*Modulo di segnalazione interna operazione sospetta*») e a trasmetterla, tramite busta chiusa "riservata", direttamente all'Unità Organizzativa Compliance e Antiriciclaggio per lo svolgimento delle analisi di propria competenza;

- ✓ ***Control Owner*:** Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Market Abuse: gestione delle operazioni sospette; Regolamento per il contrasto del Market Abuse

iii La Banca predispone, all'interno del Piano formativo per i dipendenti, un programma di formazione-informazione periodica sui reati e gli illeciti amministrativi di *market abuse* e sulle relative procedure aziendali in essere;

- ✓ ***Control Owner*:** Responsabile di Unità Organizzativa – Unità Organizzativa Formazione, selezione e relazioni sindacali- Unità Organizzativa Controlli Banca
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle Risorse umane – Formazione del personale; Regolamento per il contrasto del Market Abuse

iv Al fine di consentire l'identificazione delle operazioni potenzialmente sospette, la Banca si è dotata di un apposito strumento informatico che permette di identificare, su base giornaliera, le operazioni cosiddette "fuori misura";

- ✓ ***Control Owner*:** Unità Organizzativa Compliance e Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Procedura Market Abuse: gestione delle operazioni sospette

v La Banca prevede un processo di archiviazione per tutti gli ordini e le operazioni che sono state oggetto di analisi del Comitato Finanziario Operazioni Sospette in appositi raccoglitori. Qualora le risultanze di analisi non fossero ritenute significative vengono archiviate presso l'Unità Organizzativa Controlli Banca;

- ✓ ***Control Owner*:** Unità Organizzativa Segreteria Societaria – Unità Organizzativa Controlli Banca
- ✓ ***Documentazione interna di riferimento***: Regolamento per il contrasto del Market Abuse

vi La Banca ha adottato apposita procedura che definisce il processo di gestione, monitoraggio e trasmissione delle operazioni sospette alle Autorità di Vigilanza; all'Organismo di Vigilanza della Banca deve essere inviata puntuale informativa su tutte le operazioni sospette segnalate dalla funzione incaricata alla CONSOB;

- ✓ ***Control Owner*****:** Unità Organizzativa Compliance e Antiriciclaggio – Unità Organizzativa Controlli
- ✓ ***Documentazione interna di riferimento***: Procedura Market Abuse: gestione delle operazioni sospette

vii La Banca verifica eventuali incongruenze riportate all'interno dell'elaborazione dei dati a sistema rispetto a quanto risultante dagli altri sistemi aziendali e, in caso positivo, provvede a segnalare le anomalie riscontrate all'Unità Organizzativa Processi Banca e Canali Clienti;

- ✓ ***Control Owner*****:** Unità Organizzativa Processi Banca e Canali Clienti
- ✓ ***Documentazione interna di riferimento***: Procedura Market Abuse: gestione delle operazioni sospette

viii La Banca, per quanto concerne gli ordini disposti per conto della clientela, effettua ulteriori verifiche in merito al cliente al fine di attribuire un livello di significatività dell'operazione (*e.g.*, dati personali del cliente; Consulente Finanziario abilitato all'offerta fuori Sede di riferimento; notizia *price sensitive* associata; profilo rischio sintetico e portafoglio cliente etc.);

- ✓ ***Control Owner*****:** Unità organizzativa controlli
- ✓ ***Documentazione interna di riferimento***: Procedura Market Abuse: gestione delle operazioni sospette

ix Ciascuna Unità Organizzativa, sulla base delle proprie competenze, svolge specifiche attività di analisi e istruttorie/approfondimenti, in caso di ulteriori approfondimenti da parte del Comitato Finanziario Operazioni Sospette i merito alle operazioni sospette;

x Ciascuna Unità Organizzativa, sulla base delle proprie competenze, informano il Comitato Finanziario Operazioni Sospette sui risultati emersi a seguito dell'analisi di approfondimento richiesta da parte delle Autorità;

- ✓ ***Control Owner*****:** Unità Organizzativa competente; Comitato Finanziario Operazioni Sospette
- ✓ ***Documentazione interna di riferimento***: Procedura Market Abuse: gestione delle operazioni sospette

d) Operazioni personali aventi ad oggetto strumenti finanziari

i. La Banca individua quali sono i soggetti definiti "rilevanti" e comunica agli stessi le procedure a cui attenersi con riferimento alle disposizioni in materia di operazioni personali;

ii. La Banca prevede l'invio di una comunicazione scritta (notifica) al soggetto ritenuto rilevante che preveda al suo interno: (i) la motivazione per cui il soggetto è ritenuto rilevante; (ii) gli obblighi che i destinatari sono tenuti a rispettare (compresi i parenti del soggetto rilevante); (iii) il riepilogo delle operazioni ritenute rilevanti; (iv) le operazioni personali ritenute vietate;

iii. La Banca predispone un elenco delle operazioni personali definite come «ammesse» distinguendo quali di queste abbiano obbligo di notifica da parte del soggetto rilevante;

iv. I soggetti rilevanti sono tenuti a fornire alla Direzione Compliance e Antiriciclaggio – Unità Organizzativa Controlli Banca, tutte le informazioni relative alle operazioni personali effettuate. Le suddette informazioni devono essere notificate dai soggetti rilevanti (per il tramite di casella di posta elettronica) entro cinque giorni lavorativi dal compimento dell'operazione personale tramite l'invio di un apposito modulo.

- ✓ ***Control Owner*****: :** Direzione Compliance e Antiriciclaggio – Unità Organizzativa Controlli Banca
- ✓ ***Documentazione interna di riferimento***: Procedura Identificazione e gestione delle operazioni personali; Regolamento per il contrasto del Market Abuse

v. Le operazioni personali, notificate dai soggetti rilevanti, vengano registrate nel c.d. Registro delle operazioni personali tenuto dalla Direzione Compliance e Antiriciclaggio – Unità Organizzativa Controlli Banca;

vi. La Direzione Compliance e Antiriciclaggio – Unità Organizzativa Controlli Banca svolge, trimestralmente e tramite campionamento casuale delle operazioni segnalate, attività di monitoraggio al fine di verificare il rispetto delle disposizioni contenute in apposita procedura;

vii. La Direzione Compliance e Antiriciclaggio – Unità Organizzativa Controlli Banca svolge, tramite campionamento dei soggetti rilevanti registrati, attività di monitoraggio periodico al fine di verificare il rispetto delle disposizioni contenute in apposita procedura.

- ✓ ***Control Owner*: :** Direzione Compliance e Antiriciclaggio – Unità Organizzativa Controlli Banca
- ✓ ***Documentazione interna di riferimento***: Procedura Identificazione e gestione delle operazioni personali

9. Reati in materia di salute e sicurezza sui luoghi di lavoro

9.1. Le fattispecie di reato rilevanti di cui all'art. 25-*septies*, D.lgs. 231/2001

Occorre sottolineare, in chiave preliminare, che l'inclusione nel novero dei Reati Presupposto di fattispecie colpose – come quelle di cui all'art. 25-*septies* del Decreto – ha posto il problema della compatibilità logica tra la non volontà dell'evento, tipica degli illeciti colposi, e il finalismo sotteso al concetto di *interesse* dell'ente; ancora, è apparso assai difficile pensare, ad esempio, ad un vantaggio per l'ente connesso alla morte di un lavoratore.

Sul punto, le Sezioni Unite della Cassazione nella sentenza n. 38343 del 24 aprile 2014, emessa nell'ambito del processo cd. *Thyssen*, hanno chiarito che «*nei reati colposi di evento i concetti di interesse e vantaggio devono necessariamente essere riferiti alla condotta e non all'esito antigiuridico*». Viene chiarito che tale soluzione «*non determina alcuna difficoltà di carattere logico: è ben possibile che una condotta caratterizzata dalla violazione della disciplina cautelare e quindi colposa sia posta in essere nell'interesse dell'ente o determini comunque il conseguimento di un vantaggio. […] Tale soluzione interpretativa […] si limita ad adattare l'originario criterio d'imputazione al mutato quadro di riferimento, senza che i criteri d'ascrizione ne siano alterati. L'adeguamento riguarda solo l'oggetto della valutazione che, coglie non più l'evento bensì solo la condotta, in conformità alla diversa conformazione dell'illecito. […] È ben possibile che l'agente violi consapevolmente la cautela, o addirittura preveda l'evento che ne può derivare, pur senza volerlo, per corrispondere ad istanze funzionali a strategie dell'ente*».

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

OMICIDIO COLPOSO (ART. 589 C.P.)

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

Esempio

Allianz Bank acquista un immobile, che adibisce immediatamente a luogo di lavoro rinviando la messa a norma di taluni impianti, così da liberare entro il termine convenuto un immobile in affitto. A causa di un malfunzionamento impiantistico un Dipendente decede.

LESIONI PERSONALI GRAVI E GRAVISSIME (ART. 590, CO. 3, C.P.)

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagoni a un altro soggetto lesioni gravi o gravissime.

In particolare, ai sensi dell'art. 583, co. 1, c.p. la lesione è considerata *grave* (**i**) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni; oppure (**ii**) se il fatto produce l'indebolimento permanente di un senso o di un organo.

Ai sensi dell'art. 583, co. 2, c.p., invece, una lezione è considerata *gravissima* se dal fatto deriva (i) una malattia certamente o probabilmente insanabile; (ii) la perdita di un senso; (iii) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; (iv) la deformazione, ovvero lo sfregio permanente del viso.

Esempio

Allianz Bank acquista un immobile, che adibisce immediatamente a luogo di lavoro rinviando la messa a norma di taluni impianti, così da liberare entro il termine convenuto un immobile in affitto. A causa di un malfunzionamento impiantistico un Dipendente subisce un infortunio con prognosi di più di quaranta giorni.

9.2. Processi e attività sensibili rilevanti

In relazione ai Reati in materia di salute e sicurezza sui luoghi di lavoro, il Processo Sensibile della Banca potenzialmente più esposto al rischio è il seguente:

XIII. Adempimenti in materia di salute e sicurezza *ex* D.lgs. 81/2008

Nello specifico, all'interno del Processo Sensibile, è stata individuata la seguente Attività Sensibile:

a) Espletamento e gestione degli adempimenti in materia di tutela della salute e sicurezza sui luoghi di lavoro

- Processo Sensibile principale: **XIII**

9.3. Principi generali di comportamento

Al fine di garantire l'adozione di un valido presidio avverso la potenziale commissione dei reati di cui all'art. 25-*septies* del Decreto, la Società ha deciso di dotarsi del presente capitolo di Parte Speciale, in conformità a quanto disposto dall'art. 30 del D.lgs. 81/2008.

Nella predisposizione del presente capitolo di Parte Speciale, in particolare, la Banca ha tenuto conto dei principi cardine di cui alle Linee Guida Uni-Inail, al fine di garantire il rispetto da parte dei Destinatari di regole minime di comportamento in relazione alla determinazione della politica aziendale in tema di sicurezza, alla relativa pianificazione degli obiettivi, alla messa in atto di opportune azioni di monitoraggio, alla sensibilizzazione del personale ed, infine, al periodico riesame del sistema in essere al fine di valutarne la sua efficacia ed efficienza.

I principi generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali, ai Fornitori della Società.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*septies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

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

- il CCNL applicabile;
- il DVR con i relativi documenti integrativi;
- le procedure operative e organizzative in materia di salute e sicurezza sui luoghi di lavoro, come, ad esempio:
    - il sistema di segnalazione dei rischi;
    - quelle relative alla gestione degli appalti;
    - il sistema di sorveglianza sanitaria;
    - le modalità di consultazione del rappresentante dei lavoratori per la sicurezza;
    - il piano di emergenza.

9.4. Principi specifici per le singole attività sensibili

Con riferimento alla Attività Sensibile individuata *supra* § 9.2 si applicano i seguenti principi specifici.

9.4.1. La politica aziendale in tema di salute e sicurezza sui luoghi di lavoro

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

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

La Banca, quindi, con cadenza periodica: (i) definisce un programma di sopraluoghi in tutti i contesti aziendali in cui sussistono rischi in materia di salute e sicurezza nei luoghi di lavoro; (ii) definisce, all'interno di apposita nota operativa, un piano di interventi per l'eliminazione o la riduzione dei rischi sopra richiamati; (iii) affida agli Addetti, sotto la supervisione del Responsabile del Servizio di Prevenzione e Protezione, il controllo circa l'effettiva attuazione delle necessità di intervento indicate nella nota operativa; (iv) definisce le risorse, anche economiche, necessarie.

Principali *Control Owner* del sistema posto dalla Banca a tutela della salute e sicurezza sui luoghi di lavoro descritto nei paragrafi successivi sono: l'Unità Organizzativa Controlli; l'Unità Organizzativa Risorse Umane; il Servizio *Facility & Property Manager* di Allianz S.p.A.; l'Unità Organizzativa costituente il Servizio di Prevenzione e Protezione ed il Responsabile del Servizio di Prevenzione e Protezione; il Medico Competente; il Datore di Lavoro; Funzione Legale.

La principale documentazione interna di riferimento, invece, è la seguente:

- Procedura Presidio Specialistico di *Compliance* – Salute e Sicurezza;
- Procedura Individuazione, valutazione e misure di controllo dei rischi per la salute e la sicurezza;
- Procedura Preparazione e risposta alle emergenze;
- Procedura Gestione delle anomalie e delle azioni di miglioramento e indagine degli accadimenti pericolosi;
- Procedura Individuazione delle prescrizioni legali in ambito salute e sicurezza e gestione delle scadenze;
- Procedura Gestione indicatori in ambito salute e sicurezza;
- Procedura Gestione della sorveglianza sanitaria;
- Procedura Manuale del Sistema di Gestione Salute e Sicurezza;
- Procedura Formazione del personale;
- Procedura Gestione degli adempimenti amministrativi;
- Procedura Individuazione, valutazione e misure di controllo dei rischi per la salute e la sicurezza;
- Procedura Monitoraggio dei servizi di *Facility & Property Management* erogati da Allianz S.p.A.;

- Procedura Comunicazione, partecipazione e consultazione;
- Procedura Adempimenti in fase di definizione e sottoscrizione di contratti di acquisto di beni, servizi e prestazioni d'opera (DUVRI);
- Procedura Gestione della contrattualistica.

9.4.2. Compiti, ruoli e responsabilità delle figure rilevanti

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

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

a) Datore di Lavoro

Al Datore di Lavoro della Banca sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti compiti *non delegabili*: (i) valutare tutti i rischi per la sicurezza e la salute dei Lavoratori; (ii) elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi; (iii) designare il Responsabile del Servizio di Prevenzione e Protezione.

L'attività di valutazione e di redazione del DVR, pianificata nell'ambito della riunione periodica annuale prevista dall'art. 35 del D.lgs. 81/2008 ed effettuata anche mediante appositi sopralluoghi negli ambienti di lavoro, deve essere compiuta in collaborazione con il RSPP e con il Medico Competente.

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

La valutazione dei rischi deve essere immediatamente rielaborata, in occasione di modifiche del processo produttivo o della organizzazione del lavoro significative ai fini della salute e sicurezza dei lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione o a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità. Nelle suddette ipotesi il DVR deve essere rielaborato nel termine di trenta giorni dalla verificazione dell'evento che determina l'esigenza modificativa.

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

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

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

Si noti, comunque, che delega di funzioni non esclude l'obbligo di vigilanza in capo al Datore di Lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite.

In base alle modifiche apportate al Decreto Sicurezza dal D.lgs. 106/2009, è riconosciuta al delegato una facoltà di sub-delega delle funzioni a lui delegate, con il limite di un solo livello di sub-delega.

b) Responsabile del Servizio di Prevenzione e Protezione (RSPP)

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro si avvale, ricorrendo anche a soggetti esterni alla Banca, del Responsabile del Servizio di Prevenzione e Protezione dei rischi professionali che provvede: (i) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale; (ii) a elaborare, per quanto di competenza, le misure preventive e protettive a seguito della valutazione dei rischi e i sistemi di controllo di tali misure; (iii) a effettuare, per quanto di sua competenza, periodici sopraluoghi volti a verificare la persistente efficacia del sistema di salute e sicurezza sul lavoro, indicando in apposita nota operativa le azioni di miglioramento da attuare; (iv) a elaborare le procedure di sicurezza per le varie attività aziendali; (iv) a proporre i programmi di informazione e formazione dei Lavoratori; (v) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'art. 35 del Decreto Sicurezza; (vi) a fornire ai Lavoratori ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria.

Qualora nell'espletamento dei relativi compiti, il RSPP della Banca verificasse la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro, dovrà esserne data immediata comunicazione all'Organismo di Vigilanza.

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

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

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

c) Medico Competente

Il Medico Competente provvede, tra l'altro, a: (i) collaborare con il Datore di Lavoro e con il Responsabile del Servizio di Prevenzione e Protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori, all'attività di formazione ed informazione nei loro confronti, per la parte di competenza, e all'organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro; (ii) programmare ed effettuare la sorveglianza sanitaria; (iii) istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ogni Lavoratore sottoposto a sorveglianza sanitaria; (iv) fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informandoli sui relativi risultati; (v) comunicare per iscritto in occasione della riunione periodica di cui all'art. 3 del Decreto Sicurezza i risultati anonimi collettivi della sorveglianza sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica dei lavoratori; (vi) visitare gli ambienti di lavoro almeno a cadenza diversa in base alla valutazione di rischi.

Il Medico Competente deve essere in possesso di uno dei titoli di cui all'art. 38 D.lgs. 81/2008.

d) Rappresentante dei Lavoratori per la Sicurezza (RLS)

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

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

Il Responsabile dei Lavoratori per la Sicurezza, in particolare: (i) accede ai luoghi di lavoro; (ii) può richiedere consegna di copia del DVR (e del DUVRI) per finalità connesse all'espletamento dei compiti ad esso affidati; (iii) è consultato preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive; (iv) è consultato sulla designazione del RSPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso e del Medico Competente; (v) è consultato in merito all'organizzazione delle attività formative; (vi) promuove l'elaborazione, l'individuazione e l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei lavoratori partecipando assieme al RSPP ai sopraluoghi periodicamente organizzati al fine di valutare la persistente efficacia del sistema di SSL attuato dalla Banca; (vii) partecipa alla riunione periodica di prevenzione e protezione dai rischi; (viii) riceve informazioni inerenti la valutazione dei rischi e le misure di prevenzione relative.

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

e) Lavoratori

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

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

I lavoratori di aziende che svolgono per la Banca attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento. Nel caso di lavori in appalto, ad esempio ai sensi dell'art.26 o del Titolo IV del D.lgs. 81/2008, possono inoltre essere presenti le ulteriori figure del committente, del responsabile dei lavori, del coordinatore per la progettazione, del coordinatore per l'esecuzione: compiti e ruoli degli stessi devono essere puntualmente individuati dal contratto di appalto sottoscritto dalla Banca.

9.4.3. Sorveglianza sanitaria

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

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

- Lavoratori che utilizzano attrezzature munite di videoterminali;
- Lavoratori notturni;
- Lavoratrici in stato di gravidanza;
- Lavoratori soggetti alla movimentazioni manuale dei carichi;
- Lavoratori esposti ad eventuali agenti fisici, biologici e sostanze pericolose;
- Lavoratori esposti ad eventuali rischi da stress lavoro-correlato e mobbing.

Al fine di dare corretta attuazione all'attività di sorveglianza sanitaria da parte del Medico Competente e di consentirne una puntuale pianificazione, le competenti funzioni aziendali trasmettono al Medico Competente l'elencazione dei Lavoratori esposti ai rischi sopra evidenziati e i risultati di tale attività di sorveglianza sono registrati e archiviati secondo le modalità normativamente previste.

Di particolare rilevanza risulta essere la gestione delle attività di sorveglianza sanitaria in relazione ai seguenti aspetti: (i) trasmissione dell'elenco dei Lavoratori esposti al Medico Competente; (ii) tipologia di Lavoratori sottoposti a sorveglianza sanitaria; (iii) attività di pianificazione delle visite dei lavoratori "esposti"; (iv) struttura della relazione del Medico Competente contenente i dati relativi alla popolazione aziendale; tale relazione è parte integrante del verbale di riunione periodica ex art. 35 del Decreto Sicurezza; (v) modalità di registrazione ed archiviazione delle informazioni.

9.4.4. Informazione e formazione

L'**informazione** che la Banca riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a: (i) le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle regole adottate dalla Banca in tema di salute e sicurezza sui luoghi di lavoro; (ii) il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di sicurezza e ogni altra prescrizione relativa al sistema di salute e sicurezza sui luoghi di lavoro adottato dalla Banca, nonché ai principi indicati nel presente capitolo di Parte Speciale.

Ciò premesso, la Banca, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun Dipendente, è tenuta ai seguenti oneri informativi:

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

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

La Banca destina apposita sezione del sito intranet aziendale all'informazione su base documentale, anche mediante apposita verbalizzazione.

La Banca deve inoltre fornire adeguata **formazione** a tutti i Dipendenti in materia di salute e sicurezza sul lavoro, con specifico riferimento ai (**i**) concetti di rischio, danno, prevenzione, protezione, uso dei DPI, organizzazione della prevenzione aziendale, diritti e doveri dei vari soggetti aziendali, organi di vigilanza, controllo, assistenza; (**ii**) rischi riferiti alle mansioni (con specifico riferimento al c.d. rischio-rapina), ai possibili danni e alle conseguenti misure e procedure di prevenzione e di protezione caratteristici del settore o del comparto di appartenenza della Società; (**iii**) comportamenti da attuare nel caso in cui il rischio-rapina si concretizzi.

La suddetta attività di formazione deve essere assicurata:

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

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

- il RSPP e/o il Medico Competente devono partecipare alla stesura del piano di formazione;
- la formazione erogata deve prevedere questionari di valutazione;
- la formazione deve essere adeguata ai rischi della mansione cui il Lavoratore è in concreto assegnato;
- gli addetti a specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al pronto soccorso, RLS) devono ricevere specifica formazione;
- i Dirigenti e i Preposti ricevono a cura del Datore di Lavoro, un'adeguata e specifica formazione e un aggiornamento periodico in relazione ai propri compiti in materia di SSL; i contenuti di tale formazione comprendono:
    - principali soggetti coinvolti e i relativi obblighi;
    - definizione e individuazione dei fattori di rischio;
    - valutazione dei rischi;
    - individuazione delle misure tecniche, organizzative e procedurali di prevenzione e protezione.

La suddetta attività di formazione è attuata a seconda dei Destinatari a cui la stessa si riferisce, mediante l'organizzazione di (**i**) sedute in aula; (**ii**) corsi on-line; (**iii**) consegna di materiale didattico.

Con particolare riferimento al rischio-rapina, la formazione dei Dipendenti addetti alle filiali avviene sia mediante l'illustrazione delle misure fisiche adottate dalla Banca, quali *metal detector*, cassaforte temporizzata, rilevamenti biometrici, chiamata di emergenza), sia attraverso l'indicazione di modalità comportamentali da osservare nel caso in cui sia in corso una rapina.

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

La partecipazione all'attività di formazione è obbligatoria; la mancata partecipazione non giustificata comporterà l'applicazione del sistema sanzionatorio secondo le regole indicate nella Parte Generale del presente Modello.

9.4.5. Flussi informativi

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

A tal proposito la Banca adotta un sistema di comunicazione che prevede due differenti tipologie di flussi informativi:

- **dal basso verso l'alto** che è garantito mettendo a disposizione una casella di posta elettronica attraverso la quale ciascuno dei Lavoratori ha la possibilità di portare a conoscenza della Società osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale;
- **dall'alto verso il basso** che ha lo scopo di diffondere a tutti i Lavoratori le politiche, gli obiettivi, i programmi e i risultati in materia di salute e sicurezza sui luoghi di lavoro, incoraggiando al contempo un ritorno di informazione verso la Banca.

A tale scopo la Banca garantisce ai Destinatari un'adeguata e costante informativa attraverso la predisposizione di comunicazioni ai RLS, comunicati specifici e formali indicazioni ai Lavoratori specificamente interessati.

9.4.6. Documentazione

La Banca dovrà provvedere a conservare, sia su supporto cartaceo che informatico, i seguenti documenti: (**i**) la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente, custodita secondo le modalità concordate con il Datore di Lavoro e conservata per dieci anni; (**ii**) il Documento di Valutazione dei Rischi che contiene i programma delle misure di mantenimento e di miglioramento ed è lo strumento fondamentale che permette al Datore di Lavoro di individuare le misure di prevenzione e protezione e di pianificarne l'attuazione; (**iii**) il registro contenente le note operative, le quali indicano le azioni di miglioramento in materia di Salute e Sicurezza sul lavoro la cui necessità sia stata rilevata in occasione di sopraluoghi periodici; il registro infortuni, in cui sono annotati e descritti gli infortuni verificatisi sui luoghi di lavoro; il registro delle sanzioni, in cui sono annotate e descritte le sanzioni comminate per il caso di mancato rispetto delle prescrizioni e degli adempimenti previsti dal sistema di SSL adottato dalla Banca.

La Banca è altresì chiamata a garantire che:

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

La Banca provvede in ogni caso a conservare ogni altra documentazione e certificazione obbligatoria per legge.

9.4.7. Rispetto degli *standard* di legge relativi ad attrezzature, impianti e luoghi di lavori

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

9.4.8. Gestione delle emergenze e primo soccorso

Le situazioni d'emergenza sono gestite secondo quanto indicato nel piano di emergenza redatto, ed aggiornato a cura del Responsabile del Servizio Prevenzione e Protezione. A tal proposito si segnala che all'interno del piano di emergenza sono individuate le figure preposte alla gestione delle emergenze sia *antincendio* che di *primo soccorso*, nonché gli incaricati della gestione delle relative esercitazioni.

Secondo quanto previsto dalla normativa vigente, presso ciascuna sede aziendale, le figure identificate nel piano di emergenza organizzano un'esercitazione antincendio annuale al fine di mettere in pratica le procedure di evacuazione e di verificare la corretta applicazione delle istruzioni riportate nel piano di emergenza. Gli addetti al servizio antincendio ricevono specifica formazione circa le misure da adottare in caso si verifichi una simile emergenza.

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

9.4.9. Contratti d'appalto

La Banca deve predisporre e aggiornare l'elenco delle aziende che operano al suo interno con contratto d'appalto.

Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti in capo al Datore di Lavoro di cui all'art. 26 del Decreto Sicurezza, tra cui, in via esemplificativa:

- verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori, ai servizi e alle forniture da affidare in appalto attraverso l'acquisizione del certificato di iscrizione alla Camera di Commercio, Industria e Artigianato e l'acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'articolo 4 del Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445;
- fornire informazioni dettagliate agli appaltatori circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i Lavoratori;
- predisporre, quando necessario, il Documento Unico per la Valutazione dei Rischi da Interferenza, il quale indica le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva;
- verificare in fase di gestione del contratto ed esecuzione dei lavori il rispetto delle misure previste di prevenzione e protezione e il rispetto degli adempimenti di legge;
- assicurarsi che il personale dell'impresa appaltatrice esponga, in presenza dello specifico obbligo di legge, la tessera di riconoscimento con fotografia, dati anagrafici e indicazione del Datore di Lavoro.

Poiché gli appalti sono spesso gestiti – in forza di apposito contratto di servizi – direttamente da Allianz S.p.A., la Banca predispone apposita procedura che evidenzi la ripartizione e la modalità di attuazione degli adempimenti connessi ai contratti di appalto.

Nei contratti di somministrazione, di appalto o subappalto devono essere specificamente indicati i costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze delle lavorazioni. A tali dati possono accedere, su richiesta, il Rappresentante dei Lavoratori per la sicurezza e le organizzazioni sindacali dei lavoratori.

Infine, nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

In tutti i contratti deve essere resa nota l'adozione del Modello da parte della Banca e deve essere contenuta apposita clausola che regoli le conseguenze della violazione delle norme di cui al Decreto e delle prescrizioni del presente Modello.

9.4.10. Attività di monitoraggio

La Banca assicura un costante ed efficace monitoraggio delle misure di prevenzione e protezione adottate sui luoghi di lavoro, della loro corretta applicazione, del rispetto degli *standard* tecnico-strutturali , nonché dei principi e delle regole contenute nel presente capitolo di Parte Speciale.

A tale scopo la Banca, anche per il tramite delle funzioni e unità aziendali preposte e in coordinamento con l'Organismo di Vigilanza:

- assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro (art. 28, co. 2, lett. c), D.lgs. 81/2008), nonché la definizione dei ruoli dell'organizzazione aziendale che debbano provvedere alla loro attuazione (art. 28, co. 2, lett. d), D.lgs. 81/2008);
- assicura la presenza di tutta la documentazione necessaria per legge in materia di salute e sicurezza sui luoghi di lavoro;
- assicura un costante monitoraggio dell'adeguatezza e della funzionalità di tali misure a raggiungere gli obiettivi prefissati e della loro corretta applicazione;
- assicura un costante monitoraggio dell'attuazione delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere;
- assicura anche mediante l'attività svolta dall'Organismo di Vigilanza, un costante monitoraggio sull'adeguatezza e il rispetto delle disposizioni contenute nel presente capitolo di Parte Speciale, garantendo, ove necessario, un pronto aggiornamento.

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

- i ruoli e i compiti dei soggetti responsabili delle seguenti attività:
    - emissione di procedure e istruzioni in materia di salute e sicurezza sui luoghi di lavoro;
    - verifica del buon funzionamento degli impianti e macchinari aziendali, ivi compresi i *metal detector*, della loro manutenzione e revisione;
    - ricevimento di eventuali segnalazioni di mal funzionamento, vetustà o inefficienza di impianti o macchinari;
- l'acquisizione da parte dell'Organismo di Vigilanza, in qualunque momento e senza necessità di autorizzazione, di tutta la documentazione prodotta dalle funzioni o unità organizzative aziendali di riferimento in relazione ai controlli sulle procedure e le istruzioni di sicurezza;

- il monitoraggio sull'adeguatezza dei manuali di *security*;
- il controllo sullo svolgimento dei piani aziendali di informazione e formazione;
- l'emanazione delle istruzioni relative all'utilizzo delle attrezzature munite di videoterminali;
- il sistema sanzionatorio applicato in caso di violazione delle misure in materia di salute e sicurezza sui luoghi di lavoro.

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

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

La Banca inserisce nella programmazione annuale degli audit, interventi specifici volti a constatare il rispetto delle procedure previste dal SSL anche con riferimento agli adempimenti che – in forza di specifico contratto di servizi – sono posti in essere da Allianz S.p.A.. In tale attività, la funzione di audit interno potrà avvalersi, data l'elevata tecnicità della materia, di consulenti esterni.

La Banca prevede inoltre – con cadenza annuale – un'informativa scritta al Consiglio di Amministrazione circa il contenuto e i risultati dell'attività di monitoraggio posta in essere.

9.4.11. Riesame del sistema

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

L'attività di riesame in commento, dovrà tra l'altro basarsi su (**i**) statistiche infortuni; (**ii**) risultato dell'attività di monitoraggio effettuata; (**iii**) azioni correttive intraprese; (**iv**) rapporti sulle emergenze; (**v**) segnalazioni pervenute dall'Organismo di Vigilanza.

Della suddetta attività di riesame deve essere data evidenza su base documentale e gli esiti della stessa sono oggetto di discussione nell'ambito della riunione periodica *ex* art. 35 del Decreto Sicurezza.

9.4.12. Misure anti-contagio (COVID-19)

Il Gruppo Allianz, oltre all'aver integrato i propri DVR, ha prontamente adottato e aggiorna costantemente il «*Protocollo Anti-contagio per contrastare la diffusione del COVID-19*» che definisce le misure di prevenzione del contagio che tutti i Lavoratori, *ivi* inclusi quelli di Allianz Bank, devono rispettare.

10. Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché di autoriciclaggio

10.1. Le fattispecie di reato rilevanti di cui all'art. 25-*octies*, D.lgs. 231/2001

RICETTAZIONE (ART. 648 C.P.)

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farli acquistare, ricevere od occultare. Non è punibile a titolo di ricettazione l'autore o concorrente nel delitto presupposto.

Per *acquisto* si intende l'effetto di un'attività negoziale, a titolo gratuito ed oneroso, mediante la quale un soggetto consegua il possesso del bene. Per *ricezione* si intende ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche solo temporanea. Per *occultamento* si intende il nascondimento del bene proveniente da delitto .

Perché sussista il reato non è necessario che il denaro o i beni provengano direttamente o immediatamente dal delitto, ma è sufficiente anche una provenienza mediata, a condizione che il soggetto sia consapevole di tale provenienza.

Esempio

Il Responsabile della Unità Organizzativa Demand & Procurement Management della Banca, al fine di risparmiare sui costi delle forniture aziendali, acquista da un fornitore notoriamente coinvolto in traffici illeciti e a prezzi sensibilmente inferiori a quelli di mercato, materiale informatico di cui quest'ultimo era entrato illecitamente in possesso.

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

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

Per *sostituzione* si intende la condotta consistente nel cambiare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi. Per *trasferimento* si intende la condotta consistente nello spostamento di denaro, beni o altre utilità, anche mediante il compimento di atti negoziali.

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

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

Esempio

Un Dipendente della Banca, senza porre in essere i dovuti controlli e d'intesa con un cliente privo di adeguato capacità economica, permette allo stesso di depositare ingenti somme in denaro contante su un conto corrente e di concludere operazioni di acquisto e vendita sui mercati finanziari volte a trasferire il denaro di provenienza illecita con lo scopo di ostacolare l'identificazione della provenienza dello stesso.

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

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto. La punibilità per tale reato è prevista solo per coloro i quali non siano già compartecipi del reato principale.

Il reato non si configura se il fatto costituisce già ricettazione o riciclaggio. A differenza del riciclaggio, l'impiego non richiede che la condotta sia in grado di ostacolare l'identificazione della provenienza delittuosa del bene.

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

Esempio

Un Dipendente della Banca, senza porre in essere i dovuti controlli e d'intesa con un cliente privo di adeguata capacità economica, acquista strumenti finanziari da quest'ultimo identificati al fine di investire denaro di provenienza illecita.

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

La fattispecie è stata inserita dalla L.186/2014 al fine di superare, anche in ottemperanza ad indicazioni di fonte internazionale, uno dei principali ostacoli all'effettiva applicazione delle fattispecie fin qui esaminate, rappresentato dal cd. privilegio dell'autoriciclaggio, per effetto del quale non era punibile a titolo di riciclaggio o impiego l'autore o il concorrente nel reato presupposto.

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

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

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

Nell'ambito di attività d'impresa, pare possibile individuare taluni reati che più facilmente possono essere fonte di proventi illeciti per l'ente: così, ad esempio, i reati tributari, la truffa o la corruzione (anche tra privati). È bene precisare, tuttavia, che ai fini della sussistenza della responsabilità dell'ente non si richiede che i proventi derivino da reati presupposto di una responsabilità dell'ente: il reato presupposto della responsabilità amministrativa dell'ente è infatti il reato di autoriciclaggio, non i reati presupposto di tale reato.

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

Esempi

Il Chief Financial Officer *di Allianz Bank, al fine di consentire l'abbattimento dell'imponibile della Banca, indica in dichiarazione costi inesistenti. Successivamente investe per conto della Società i proventi del reato tributario in prodotti finanziari con operazioni concretamente idonee ad ostacolare la tracciabilità.*

10.2. La normativa in materia di prevenzione del riciclaggio: cenni.

La normativa italiana in tema di prevenzione del fenomeno del riciclaggio prevede norme tese ad ostacolare le pratiche di riciclaggio, vietando tra l'altro l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati in appositi archivi.

Nello specifico, il corpo normativo in materia di riciclaggio è costituito anzitutto dal D.lgs. 231/2007.

Il Decreto Antiriciclaggio – tra i cui destinatari figura anche la Banca (si v. *infra*) – intende essenzialmente prevenire il rischio che il sistema finanziario sia utilizzato per il compimento di operazioni di riciclaggio e, a tal fine, pone a carico dei destinatari una serie di obblighi, il cui inadempimento è sanzionato, in alcuni casi, anche penalmente.

Proprio in considerazione della sua finalità preventiva, il D.lgs. 231/2007 dà una definizione molto ampia della nozione di riciclaggio: tale definizione, ricomprende anche condotte che integrerebbero fattispecie di reato diverse dal riciclaggio, o che sarebbero prive di sanzione penale. È importante precisare che è alla nozione "amministrativa" di riciclaggio che la legge ricollega il sorgere di tutti gli obblighi di natura preventiva e degli obblighi di collaborazione attiva disciplinati dal decreto stesso. Ai fini, invece, della responsabilità penale degli enti è necessario fare riferimento alle fattispecie di reato sopra esaminate, previste dal codice penale.

Non vi è dubbio, peraltro, che il puntuale rispetto di tutti gli obblighi imposti dal D.lgs. 231/2007 sia indispensabile sotto il profilo della valutazione di adeguatezza del Modello ai fini della prevenzione del rischio riciclaggio. Benché l'inadempimento degli obblighi "antiriciclaggio", anche nei casi in cui sia penalmente sanzionato, non sia idoneo a far sorgere una responsabilità dell'ente, in alcuni casi l'omesso rispetto degli obblighi "antiriciclaggio" (ad esempio, l'omessa segnalazione di operazione sospetta) potrebbe addirittura configurare, secondo talune pronunce giurisprudenziali, un concorso in una condotta di riciclaggio a carico dell'autore della violazione.

Il Decreto Antiriciclaggio prevede in sostanza i seguenti strumenti di contrasto del fenomeno del riciclaggio di proventi illeciti:

A. la previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (vaglia postali, certificati di deposito, ecc.) in euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiore a € 2.000 (il limite è valido dal 1 luglio 2020 al 31 dicembre 2021; salvo ulteriori interventi normativi, poi, lo stesso passerà dal 1 gennaio 2022 a € 1.000). Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.;

B. gli obblighi di adeguata verifica della clientela (elencati dagli artt. 17-30 del Decreto Antiriciclaggio) dai soggetti individuati dall'art. 3 del medesimo decreto in relazione ai rapporti ed alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi. In tale ambito rientra anche l'obbligo della clientela di fornire, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate per consentire agli intermediari di adempiere agli obblighi di adeguata verifica;

C. l'obbligo di astenersi *ex* art. 42 del Decreto Antiriciclaggio dall'apertura del rapporto continuativo, dall'esecuzione dell'operazione ovvero di porre fine al rapporto continuativo già in essere, qualora l'intermediario non sia in grado di rispettare gli obblighi di adeguata verifica della clientela;

D. gli obblighi di conservazione (elencati dagli artt. 31-34 del Decreto Antiriciclaggio) di documenti o le copie degli stessi e registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;

E. gli obblighi di segnalazione (elencati dagli artt. 35-41 del Decreto Antiriciclaggio) all'UIF di tutte quelle operazioni, poste in essere dalla clientela, ritenute *sospette* e cioè quando tali soggetti sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo; in particolare, devono intendersi sospette quelle operazioni che per caratteristiche, entità, natura o per qualsivoglia altra circostanza inducano a ritenere che il denaro, i beni e le utilità oggetto delle operazioni medesime possano provenire dalla commissione di reati in genere. Seguendo l'elenco previsto dalle istruzioni operative per l'individuazione di operazioni sospette emesse da Banca d'Italia, si indicano a titolo esemplificativo quali possibili indici di anomalia:

- ripetute operazioni della stessa natura non giustificate dall'attività svolta dal cliente ed effettuate con modalità tali da denotare intenti dissimulatori (per esempio, frequenti afflussi di disponibilità finanziarie trasferite dopo un breve lasso di tempo con modalità o destinazioni non ricollegabili alla normale attività del cliente; alimentazione dei rapporti con strumenti che non appaiono coerenti con l'attività svolta dal cliente);

- operazioni di ingente ammontare che risultano inusuali rispetto a quelle di norma effettuate dal cliente, soprattutto se non vi sono plausibili giustificazioni economiche o finanziarie;
- ricorso a tecniche di frazionamento dell'operazione idonee ad eludere gli obblighi di identificazione e registrazione;
- operazioni con configurazione illogica, soprattutto se risultano svantaggiose per il cliente sotto il profilo economico o finanziario;
- operazioni effettuate frequentemente da un cliente in nome o a favore di terzi, qualora i rapporti non appaiano giustificati;
- operazioni con controparti insediate in Paesi non aderenti al GAFI o noti come centri *off-shore* o come zone di traffico di stupefacenti o di contrabbando di tabacchi che non siano giustificate dall'attività economica del cliente o da altre circostanze;
- operazioni richieste con indicazioni palesemente inesatte o incomplete, tali da far ritenere l'intento di occultare informazioni essenziali, soprattutto se riguardanti i soggetti interessati all'operazione;
- prelevamento di denaro contante per importi rilevanti, salvo che il cliente non rappresenti particolari esigenze;
- versamento di denaro contante per importi rilevanti, non giustificabile con l'attività economica del cliente;
- ricorso al contante in sostituzione degli usuali mezzi di pagamento utilizzati dal cliente.

Ai sensi dell'art. 3 del Decreto Antiriciclaggio, i soggetti sottoposti agli obblighi sopra richiamati, tra gli altri, sono:

- gli **intermediari finanziari** e gli altri soggetti esercenti attività finanziaria, tra cui:
  - Poste Italiane S.p.a.;
  - Cassa Deposito e Prestiti S.p.a.;
  - le banche;
  - le società di intermediazione mobiliare (SIM);
  - le società di gestione del risparmio (SGR);
  - le società di investimento a capitale variabile (SICAV);
- i **professionisti**, tra i quali si ricordano:
  - i dottori commercialisti;
  - i notai e gli avvocati quando, in nome e per conto dei propri clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i propri clienti nella predisposizione o nella realizzazione delle altre operazioni indicate dall'art. 3, co. 4, lett. c) del Decreto Antiriciclaggio;
  - i revisori legali.

10.3. Processi e attività sensibili rilevanti

In relazione ai Reati di cui all'art. 25-*octies* del Decreto, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

II. Gestione dei flussi monetari e finanziari;

IV. Formazione del bilancio e gestione degli adempimenti societari e dei rapporti con gli organi di controllo;

V. Commercializzazione di prodotti bancari, finanziari e assicurativi;

VII. Acquisto di beni, servizi e consulenze;

XVII. Gestione della fiscalità aziendale.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Esecuzione di verifiche in fase di accensione di rapporti anche attraverso canali fisici

- Processo Sensibile principale: **V**

b) Esecuzione di operazioni disposte dalla clientela

- Processo Sensibile principale: **V**

c) Acquisto di beni, servizi e consulenze

- Processo Sensibile principale: **II, VII**

d) Gestione della contabilità generale

- Processo Sensibile principale: **IV**

e) Gestione della fiscalità aziendale

- Processo Sensibile principale: **XVII**

10.4. Principi generali di comportamento

La Banca da sempre dedica particolare attenzione e cautela ai processi che regolano le attività tipiche dell'offerta dei propri servizi bancari e di investimento, nonché della gestione dei patrimoni affidati, ciò anche al fine di monitorare quei comportamenti che possono essere messi in correlazione con attività illecite connesse ai reati di riciclaggio e di finanziamento al terrorismo.

In particolare, la Banca applica nelle attività sensibili di cui alla presente Parte Speciale le norme ed i precetti di legge e regolamenti rilevanti, quali le disposizioni del Decreto Antiriciclaggio le regole ed i principi contenuti nelle Istruzioni Operative per l'Individuazione di Operazioni Sospette emanate da Banca d'Italia.

I principi generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali, ai Consulenti, ai *Partner* e agli Intermediari assicurativi della Società.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*octies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

Al fine di mitigare il rischio di commissione dei reati di riciclaggio e del finanziamento al terrorismo, di conseguenza, anche assicurare il corretto adempimento degli obblighi connessi alla normativa antiriciclaggio, la Banca, in relazione ai rapporti continuativi ed alle operazioni inerenti lo svolgimento della propria attività istituzionale o professionale, assolve i seguenti **obblighi**, già per altro verso osservati in ottemperanza alla normativa in vigore:

- identificare la clientela, in particolare nei seguenti casi: (**i**) instaurazione di un rapporto continuativo; (**ii**) esecuzione di operazioni di importo pari o superiore a € 15.000, sia nel caso di un'unica operazione, sia nel caso di più operazioni che appaiano collegate o frazionate; (**iii**) acquisizione o modifica di soggetti delegati ad operare sullo stesso rapporto; (**iv**) in sede di chiusura del rapporto continuativo, qualora sia disposta da un soggetto in precedenza non identificato. Pertanto, il soggetto da identificare può essere, a seconda dei casi:

- colui che compie l'operazione (ovvero chi si presenta fisicamente allo sportello o ad un incaricato della Banca), sia titolare del conto, un suo delegato e/o procuratore, esibitore e/o presentatore, anche se il documento di cassa sia già sottoscritto dal titolare del rapporto;
- colui che compie l'operazione dichiarando espressamente di agire per conto di un terzo. In tal caso si consideri, p.e., (a) se il soggetto non è legato al terzo da alcun rapporto: chi agisce deve indicare per iscritto sotto la propria personale responsabilità le complete generalità del soggetto per conto del quale esegue l'operazione; (b) se il soggetto è legato al terzo in quanto delegato, procuratore, esibitore, presentatore che ha con l'ordinante un rapporto di dipendenza nel caso o in cui il soggetto (titolare, delegato, etc.) sia già censito – è sufficiente comunicare il nome e cognome di chi effettua l'operazione e gli estremi del rapporto; ovvero, nel caso in cui il soggetto non sia ancora censito – chi agisce andrà censito secondo le modalità di cui alla procedura interna adottata dalla Banca;
- colui che accende, estingue nonché varia un conto, deposito o altro rapporto continuativo, nominativo o al portatore, in denaro o in titoli, di qualunque importo (detti rapporti devono essere intesi quali "conti movimentabili", ossia che possono dar luogo ad operazioni di versamento, prelievo o trasferimento di denaro e di altri valori; inoltre devono sussistere i requisiti del "rapporto contrattuale di durata");
- per le persone giuridiche (da intendersi tutte quelle che sono diverse dalle persone fisiche e dalla ditta individuale) si dovrà identificare sia l'ente (denominazione, ragione sociale, sede, codice fiscale), che il legale rappresentante o, in ogni caso, il soggetto (o i soggetti) che procede all'apertura del rapporto, purché fornito di adeguati poteri, nonché i soggetti delegati ad operare sul conto.

- gestire correttamente l'AUI, Archivio Unico Informatico, istituito presso la Banca, sul quale dovranno essere registrati e conservati i dati identificativi e le altre informazioni relative alle operazioni ed ai rapporti continuativi. La registrazione potrà avvenire contestualmente all'operazione o in un momento successivo, entro e non oltre trenta giorni dalla data dell'operazione;
- inviare mensilmente i dati aggregati all'UIF, Unità di Informazione Finanziaria;
- valutare la clientela in funzione del rischio potenziale di commissione dei reati di riciclaggio e di finanziamento del terrorismo sulla base della conoscenza della clientela e secondo un criterio che tenga conto degli aspetti di carattere oggettivo e soggettivo legati alla clientela, considerando anche le liste di evidenza accentrate e predisponendo controlli rafforzati per determinate categorie di soggetti;
- segnalare tempestivamente le operazioni sospette all'UIF, anche nel caso in cui le stesse siano rifiutate o comunque non concluse. Tale obbligo sussiste per l'intera durata del rapporto e non si intende limitato alle sole fasi di instaurazione o di chiusura del rapporto.

10.5. Principi specifici per le singole attività sensibili

Con riferimento alle Attività Sensibili individuate *supra* §10.3, si applicano i seguenti principi.

a) Esecuzione di verifiche in fase di accensione di rapporti anche attraverso canali fisici; e

b) Esecuzione di operazioni disposte dalla clientela

VALUTAZIONE DELLA CLIENTELA IN FUNZIONE DEL RISCHIO RICICLAGGIO

i La Banca anche per il tramite delle unità operative più esposte ai contatti con la clientela (*e.g.*, i Consulenti Finanziari abilitati all'offerta fuori sede e gli addetti allo sportello), valuta le informazioni fornite dai clienti, tra le quali anche quelle relative al titolare effettivo, al fine di determinare i profili di "rischio riciclaggio e di finanziamento del terrorismo" connessi con ciascun cliente. A tal fine, il soggetto competente

nell'ambito dell'unità operativa interessata riceve dal cliente le informazioni attraverso le quali consentire alla Banca di effettuare una classificazione della clientela in base al rischio. Le informazioni raccolte dalla clientela sono analizzate e conservate nel dossier di ciascun cliente, secondo quanto stabilito dalle procedure adottate dalla Banca.

La valutazione del profilo può fondarsi sui seguenti "elementi di attenzione":

- settore di attività e professione del cliente/settore di attività ed oggetto sociale (in caso di persona giuridica) che possono comportare l'utilizzo di contanti e titoli al portatore;
- operatività canalizzata da conti correnti esteri;
- operatività attraverso società fiduciarie/procuratori/delegati/mandatari;
- operatività per il tramite di soggetto giuridico la cui proprietà non è trasparente, ossia è detenuta da altri veicoli societari la cui proprietà non è identificabile;
- residenza/sede sociale del cliente in "paradisi fiscali" o individuati dal Gruppo di Azione Finanziaria contro il riciclaggio di danaro (GAFI) come "non cooperativi".

Nel valutare e nell'aggiornare il profilo del cliente dovranno altresì essere presi in considerazione gli indici di anomalia rilevanti al fine della segnalazione delle operazioni sospette, così come meglio specificate nel successivo punto con riferimento all'uso del contante e titoli al portatore.

Una volta effettuata la valutazione di tutti gli elementi sopra indicati, i clienti della Banca saranno suddivisi nelle categorie previste dalle procedure interne della Banca.

ii Il Responsabile Centrale Antiriciclaggio, periodicamente, per il tramite delle funzioni aziendali a contatto con la clientela, dovrà valutare la necessità di modificare il profilo di rischio attribuito ad ogni singolo cliente e dei risultati di tale attività dovrà essere fornita opportuna comunicazione all'Organismo di Vigilanza, così come previsto dalle procedure interne della Banca;

iii Periodicamente e seguendo apposita procedura, la Banca valuterà l'opportunità di continuare il proprio rapporto contrattuale con soggetti appartenenti alla categoria "a rischio alto", dandone opportuna comunicazione all'Organismo di Vigilanza;

iv Le procedure interne prevedono i casi in cui la Banca si astiene obbligatoriamente dall'apertura del rapporto o dall'esecuzione dell'operazione, qualora non sia in grado di rispettare gli obblighi di adeguata verifica della clientela. Inoltre, tali procedure interne prevedono le modalità per l'ottenimento dalla clientela delle informazioni sullo scopo e sulla natura del rapporto continuativo instaurato;

v La Banca adotta presidi idonei a garantire in presenza di un rischio elevato di riciclaggio, l'adempimento degli obblighi di adeguata verifica rafforzata della clientela;

vi La Banca si dota di presidi in grado di garantire un costante monitoraggio del profilo di rischio assegnato a ciascun cliente;

vii La Banca destina apposito spazio all'interno dell'intranet aziendale in cui vengono pubblicate e costantemente aggiornate la normativa in materia di antiriciclaggio e le procedure aziendali adottate in materia.

- ✓ ***Control Owner*:** Unità Organizzativa Antiriciclaggio
- ✓ ***Documentazione interna di riferimento***: Manuale Antiriciclaggio; Procedura Organizzativa Controlli Antiriciclaggio; Codice Anticorruzione Gruppo Bancario Allianz Bank

USO DEL CONTANTE E TITOLI AL PORTATORE

i La Banca non può fare da tramite nei trasferimenti di denaro contante o di titoli al portatore tra soggetti diversi qualora l'importo del trasferimento sia complessivamente pari o superiore ad € 2.000. I moduli di assegni bancari rilasciati dalla Banca, salvo che il cliente ne richieda per iscritto la forma libera, devono riportare la clausola di non trasferibilità. Qualora gli assegni bancari siano emessi per importi pari o superiori ad € 1.000, devono recare l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità.

ii Gli assegni circolari devono essere ammessi con l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità. Qualora l'importo dell'assegno circolare rilasciato sia inferiore all'importo previsto dalla normativa vigente, il cliente può richiedere per iscritto che lo stesso non contenga la clausola di non trasferibilità.

SEGNALAZIONE DELLE OPERAZIONI SOSPETTE

i Sono sospette quelle operazioni che per caratteristiche, entità, natura o per qualsivoglia altra circostanza inducano a ritenere che il denaro, i beni e le utilità oggetto delle operazioni medesime possano provenire da reati di riciclaggio. Per l'elenco completo degli indici di anomalia previsti dalle istruzioni operative per l'individuazione di operazioni sospette emesse da Banca d'Italia, si rinvia alla procedura aziendale interna adottata dalla Banca

ii In presenza di un'operazione sospetta, l'unità operativa interessata secondo la procedura adottata dalla Banca, deve farne tempestiva segnalazione all'Ufficio Antiriciclaggio, il quale avrà il compito di: (i) analizzare la documentazione relativa all'operazione segnalata dall'unità operativa interessata, verificando la sussistenza dei presupposti problematici alla base della segnalazione, anche riscontrando l'operazione con il profilo economico sociale del cliente e l'eventuale esistenza di evidenze preesistenti nel sistema GIANOS (Generatore Indici Anomalia per Operazioni Sospette) riconducibili al medesimo soggetto segnalato; (ii) sottoporre l'operazione alla valutazione del Responsabile Centrale Antiriciclaggio, il quale, a sua volta, dovrà effettuare una sua propria valutazione degli elementi alla base dell'operazione oggetto di segnalazione.

iii Il Responsabile Centrale Antiriciclaggio, compiuta una prima analisi del profilo problematico dell'operazione, la sottoporrà, insieme ai propri commenti sullo stesso, al Responsabile Aziendale Antiriciclaggio per un'ultima valutazione.

iv Se viene confermata anche a questo livello la volontà di far proseguire la segnalazione, il Responsabile Aziendale Antiriciclaggio ritrasmetterà la stessa all'Ufficio Antiriciclaggio, con il corredo completo della documentazione cartacea. L'Ufficio Antiriciclaggio predisporrà la segnalazione sull'apposito modulo informatico e la invierà all'UIF.

TIPOLOGIA DELLE OPERAZIONI

v Ad ulteriore specificazione, ogni operazione dovrà essere effettuata sulla base delle procedure che si fondano sui seguenti principi: (a) non è necessario procedere all'identificazione diretta nei casi in cui ai clienti sia stata rilasciata attestazione da soggetti presso i quali gli stessi sono titolari di conti, depositi o altri rapporti continuativi e in relazione ai quali sono stati già identificati di persona; (b)nel caso di bonifici, l'identificazione andrà effettuata sia dalla Banca dell'ordinante che da quella del beneficiario, le quali dovranno registrare l'operazione nell'archivio unico informatico e mantenere memoria dei dati d'archivio per i dieci anni prescritti. Andranno registrati anche i dati della "controparte" per cui ciascun intermediario dovrà comunicare all'altro tali dati; (c) nel caso di ordini di pagamento o accreditamento provenienti dall'estero, l'intermediario italiano incaricato dovrà registrare le complete generalità del beneficiario, l'intermediario estero intervenuto per conto dell'ordinante e, ove noti, il Paese e le generalità di quest'ultimo; (d) nel caso in cui le operazioni vengano eseguite sulla base di ordini di pagamento o accreditamento, la società che cura il trasferimento ha l'obbligo di registrare l'operazione.

✓ ***Control Owner***: Unità Organizzativa Compliance e Antiriciclaggio e Unità Organizzativa Antiriciclaggio

- ✓ ***Documentazione interna di riferimento***: Manuale Antiriciclaggio; Procedura Organizzativa Controlli Antiriciclaggio; Codice Anticorruzione Gruppo Bancario Allianz Bank

c) Acquisto di beni, servizi e consulenze

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. g) della Parte Speciale).

d) Gestione della contabilità; e

e) Gestione della fiscalità aziendale

Si rinvia a quanto previsto nel capitolo relativo ai Reati tributari (§15.4, lett. d) e lett. f) della Parte Speciale).

11. Reati in materia di violazione del diritto d'autore

11.1. Le fattispecie di reato rilevanti di cui all'art. 25-*novies*, D.lgs. 231/2001

DIVULGAZIONE TRAMITE RETI TELEMATICHE DI UN'OPERA DELL'INGEGNO PROTETTA (ART. 171, L. 633/1941)

In relazione alle fattispecie delittuose di cui all'art. 171 della L. 633/1941, costituiscono presupposto di una responsabilità dell'ente esclusivamente le seguenti condotte: (**i**) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa; (**ii**) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Esempio

Un Dirigente della Banca ordina che siano caricati sulla rete aziendale dei contenuti coperti dal diritto d'autore affinché gli stessi possano essere utilizzati nell'ambito dell'attività lavorativa.

DUPLICAZIONE DI PROGRAMMI INFORMATICI O IMPORTAZIONE, DISTRIBUZIONE, VENDITA, DETENZIONE PER FINI COMMERCIALI O IMPRENDITORIALI DI PROGRAMMI CONTENUTI IN SUPPORTI NON CONTRASSEGNATI DALLA SIAE (ART. 171-*BIS*, L. 633/1941)

La norma in esame è volta a tutelare il corretto utilizzo dei software e delle banche dati. Per ciò che concerne i *software*, ai sensi del primo comma, il reato si configura nel caso in cui taluno abusivamente duplichi, per trarne profitto, programmi per elaboratore o ai medesimi fini importi, distribuisca, venda, detenga a scopo commerciale o imprenditoriale o conceda in locazione programmi contenuti in supporti non contrassegnati dalla SIAE. Il fatto è punito anche se la condotta ha a oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. Per ciò che concerne le *banche dati*, il secondo comma della stessa norma punisce chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduca, trasferisca su altro supporto, distribuisca, comunichi, presenti o dimostri in pubblico il contenuto di una banca dati ovvero esegua l'estrazione o il reimpiego della banca dati, o, ancora, distribuisca, venda o conceda in locazione una banca dati in violazione delle disposizioni di cui alla legge sul diritto d'autore.

Sul piano soggettivo, per la configurabilità del reato si richiede lo specifico scopo di conseguire un guadagno di tipo anche non prettamente economico (fine di profitto).

Esempio

Un Dirigente della Banca decide di far installare sui computer in dotazione dei Dipendenti programmi "pirata".

DUPLICAZIONE, RIPRODUZIONE E TRASMISSIONE DI UN'OPERA DELL'INGEGNO DESTINATA AL CIRCUITO TELEVISIVO, CINEMATOGRAFICO, DELLA VENDITA O DEL NOLEGGIO (ART. 171-*TER*, L. 633/1941)

La disposizione in esame tutela una serie numerosa di opere dell'ingegno nei confronti di condotte abusive variamente descritte: opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali, ma anche opere letterarie, scientifiche o didattiche. A restringere l'ambito di applicabilità della disposizione, però, vi sono due requisiti: il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno e il secondo è il fine di lucro.

Esempio

La Banca, per una campagna pubblicitaria, utilizza abusivamente un'opera musicale protetta dal diritto d'autore.

11.2. Processi e attività sensibili rilevanti

In relazione ai Reati di cui all'art. 25-*novies* del Decreto, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

V. Commercializzazione dei prodotti bancari, finanziari e assicurativi;

XI. Utilizzo dei sistemi informativi aziendali;

XVI. Gestione e rispetto della proprietà industriale e intellettuale.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Utilizzo degli applicativi informatici aziendali

- Processi Sensibili principali: **XI** e **XVI**

b) Gestione del sito internet aziendale

- Processi Sensibili principali: **XI** e **XVI**

c) Pubblicizzazione dei prodotti bancari, finanziari e assicurativi

- Processi Sensibili principali: **V** e **XVI**

11.3. Principi generali di comportamento

I principi generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché ai Consulenti Finanziari abilitati all'offerta fuori sede.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*novies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

In particolare, è fatto divieto di utilizzare illecitamente materiale tutelato dall'altrui diritto d'autore.

11.4. Principi specifici per le singole attività sensibili

Con riferimento alle Attività Sensibili individuate *supra* §11.2, si applicano i seguenti principi.

a) Utilizzo degli applicativi informatici aziendali

i Allianz Bank adotta misure specifiche che impediscano l'installazione e l'utilizzo di *software* non approvati dalla Banca, non correlati con la Banca, non correlati con l'attività professionale espletata per la stessa o per il quali non si possiede la necessaria licenza d'uso;

ii La Banca richiama periodicamente in modo inequivocabile i propri Dipendenti, anche attraverso apposita attività di formazione, a un corretto utilizzo degli strumenti informatici in proprio possesso;

iii La Banca predispone e dispone adeguate difese a protezione dei sistemi informatici aziendali;

- ✓ ***Control Owner***: Unità Organizzativa *Information Security Office*; Unità Organizzativa Organizzazione e Sviluppo Applicativo
- ✓ ***Documentazione interna di riferimento***: Allianz *Information Security Directives*; Procedura Gestione degli incidenti di sicurezza informatica; Procedura Gestione dei cambiamenti; Procedura Gestione delle applicazioni sviluppate dalle unità operative di controllo; Procedura Gestione e controllo degli accessi; Procedura dei controlli sull'operatività degli *outsourcer* informatici

iv La Banca emana istruzioni alle competenti funzioni interne affinché sia rispettata la corrispondenza tra software in uso e numero di licenze d'uso ottenute;

v La Banca richiama l'attenzione ai destinatari circa la necessità che nelle fasi di sviluppo "interno" di software precedentemente acquistati dalla Banca, non vengano violati diritti di proprietà intellettuale altrui.

- ✓ ***Control Owner***: Unità Organizzativa *Information Security Office*; Unità Organizzativa Organizzazione e Sviluppo Applicativo
- ✓ ***Documentazione interna di riferimento***: Allianz *Information Security Directives*; Procedura Gestione degli incidenti di sicurezza informatica; Procedura Gestione dei cambiamenti; Procedura Gestione delle applicazioni sviluppate dalle unità operative di controllo

vi La Banca adotta presidi analoghi a quelli previsti per la gestione del sito internet anche con riferimento alla gestione del centralino telefonico aziendale, ciò in ragione del rischio connesso all'eventuale utilizzazione di composizioni musicali in violazione della normativa applicabile nelle fasi in cui il cliente è posto "in attesa".

- ✓ ***Control Owner*****:** Direzione Marketing, Unità Organizzativa Call Center
- ✓ **Documentazione interna di riferimento**: Procedura Comunicazione esterna, pubblicitaria e promozione della clientela

b) Gestione del sito internet aziendale

i La Banca disciplina formalmente le modalità attraverso le quali modificare il sito internet aziendale;

ii La Banca indica quali figure interne partecipino al processo decisionale di modifica del sito internet aziendale e quali figure siano invece demandate ad attuare effettivamente le modifiche, prevedendo, ove necessario, una preventiva consultazione della Funzione Legale;

iii La Banca prevede che l'accesso al sito internet aziendale a fini di modifica sia attuabile solo in possesso di specifiche *password* a tale scopo generate;

iv La Banca fornisce alle figure aziendali interessate adeguata informazione circa le potenziali rischiosità in materia di responsabilità amministrativa degli enti connesse all'attività di configurazione del sito internet aziendale;

v La Banca emana istruzioni alle competenti funzioni interne affinché all'interno del sito internet venga utilizzato materiale coperto da altrui diritto d'autore solamente in presenza di un diritto all'utilizzazione dello stesso;

vi La Banca verifica periodicamente l'eventuale pubblicazione sul proprio sito internet aziendale di materiale non autorizzato.

- ✓ ***Control Owner*****:** Unità Organizzativa Comunicazione Esterna
- ✓ **Documentazione interna di riferimento**: Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa-Funzionigramma; Procedura Comunicazione esterna, pubblicitaria e promozionale alla clientela

c) Pubblicizzazione dei prodotti bancari, finanziari, assicurativi

i La Banca emana istruzioni alle competenti funzioni interne affinché in occasione delle campagne pubblicitarie venga utilizzato materiale coperto da altrui diritto d'autore solamente in presenza di un diritto all'utilizzazione dello stesso;

ii La Banca verifica periodicamente l'eventuale utilizzo in occasione delle campagne pubblicitarie di materiale non autorizzato.

- ✓ ***Control Owner*****:** Direzione Marketing, Unità Organizzativa Organizzazione Eventi; Unità Organizzativa Legale; Unità Comunicazione esterna
- ✓ **Documentazione interna di riferimento**: Procedura Comunicazione esterna, pubblicitaria e promozionale alla clientela

12. Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

12.1. La fattispecie di reato rilevante di cui all'art. 25-*decies*, D.lgs. 231/2001

INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 377-*BIS* C.P.)

Il delitto di cui all'art. 377-*bis* del codice penale sanziona – salvo che il fatto costituisca reato più grave – «*chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere*».

Esempio

Un Amministratore della Banca offre denaro a un Dirigente della Banca sottoposto a indagini, al fine di indurlo ad avvalersi della facoltà di non rispondere nel corso di un interrogatorio davanti all'autorità giudiziaria.

12.2. Processo e attività sensibile rilevanti

In relazione al Reato di cui all'art. 25-*decies* del Decreto, il Processo Sensibile della più esposto al rischio di commissione di illeciti è il seguente:

X. Gestione del contenzioso.

Nello specifico, all'interno dei singolo Processo Sensibile, è stata individuata la seguente Attività Sensibile:

a) Gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere, indagati o imputati in un procedimento penale, nell'ambito delle cause di varia natura nelle quali la Società risulti coinvolta

- Processo Sensibile principale: **X**

12.3. Principi generali di comportamento

I principi generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali, ai Consulenti della Banca.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino la fattispecie di reato contemplata nell'art. 25-*decies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

In particolare, è fatto espresso divieto ai Destinatari, di ricorrere alla forza fisica, a minacce o all'intimidazione oppure promettere, offrire o concedere un'indebita utilità per indurre colui il quale può avvalersi della facoltà di non rispondere nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all'autorità giudiziaria, con l'intento di ottenere una pronuncia favorevole alla Società o determinare il conseguimento di altro genere di vantaggio.

Nell'ambito dei suddetti comportamenti è fatto ulteriormente divieto di: (**i**) usare qualsiasi forma di violenza o minaccia al fine di indurre una persona chiamata a rendere dichiarazioni davanti all'autorità giudiziaria a non rendere tali dichiarazioni o a rendere dichiarazioni mendaci; (**ii**) offrire o promettere di offrire denaro o altra utilità al fine di indurre una persona chiamata a rendere dichiarazioni davanti all'autorità giudiziaria a non rendere tali dichiarazioni o a rendere dichiarazioni mendaci.

12.4. Principi specifici per la singola attività sensibile

Con riferimento all'Attività Sensibile individuata *supra* §12.2, si applicano i seguenti principi:

a) Gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere, indagati o imputati in un procedimento penale, nell'ambito delle cause di varia natura nelle quali la Società risulti coinvolta

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5(n) della Parte Speciale).

13. Reati ambientali

13.1. Le fattispecie di reato rilevanti di cui all'art. 25-*undecies*, D.lgs. 231/2001

INQUINAMENTO AMBIENTALE DOLOSO E COLPOSO (ART. 452-*BIS* C.P. E ART. 452-*QUINQUIES* C.P.)

Il reato previsto dall'art. 452-*bis* c.p. punisce chiunque, abusivamente, cagioni una compromissione o un deterioramento significativi e misurabili dello stato preesistente delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo oppure di un ecosistema, della biodiversità, anche agraria, della flora o della fauna. Il secondo comma prevede un'ipotesi aggravata quando il delitto sia commesso in un'area naturale protetta o sottoposta a specifici vincoli, ovvero in danno di specie animali o vegetali protette.

La norma in esame punisce l'inquinamento ambientale, ovvero quelle condotte che, pur senza determinare un evento catastrofico dotato dei requisiti del disastro (ovvero vastità del fenomeno e messa in pericolo di un numero indeterminato di persone), siano comunque altamente lesive per il bene dell'ambiente. Il bene giuridico ambiente descrive infatti una nozione intermedia, mediante la punibilità sia per la mera lesione dell'equilibrio ambientale, sia qualora sia coinvolta la vita umana.

Il reato di cui all'art. 452-*quinquies* c.p. punisce chiunque cagioni, per colpa, il delitto di inquinamento ambientale (o di disastro ambientale di cui all'art. 452-*quater* c.p.), operando una diminuzione della pena. Al secondo comma è prevista una ulteriore diminuzione di pena qualora non venga cagionato un vero e proprio inquinamento o disastro ambientale, ma un mero pericolo (da doversi accertare in concreto) che essi si realizzano.

Esempio

La Banca affida il servizio di smaltimento dei propri rifiuti ad un operatore esterno, che pratica prezzi significativamente più bassi rispetto a quelli di mercato sapendo che questi interra i rifiuti raccolti in una cava non destinata allo smaltimento, così cagionando l'inquinamento del sottosuolo.

ATTIVITÀ ORGANIZZATE PER IL TRAFFICO DI RIFIUTI (ART. 452-*QUATERDECIES* C.P.)

Ai sensi dell'art. 452-*quaterdecies*, comma primo, c.p. è punito chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti. Il reato è aggravato qualora i rifiuti siano ad alta radioattività, secondo quanto previsto dall'art. 452-*quaterdecies*, comma 2, c.p.

Esempio

La Banca, impegnata nella ristrutturazione di un nuovo immobile di sua proprietà, si organizza con una società terza al fine di cederle sistematicamente ingenti quantitativi di rifiuti da smaltire abusivamente.

GESTIONE NON AUTORIZZATA DI RIFIUTI (ART. 256, CO. 1, D.LGS. 152/2006)

Il primo comma dell'art. 256 D.lgs. 152/2006 punisce una pluralità di condotte connesse alla gestione non autorizzata dei rifiuti, ossia le attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti di qualsiasi genere – pericolosi e non pericolosi – poste in essere in mancanza della specifica autorizzazione, iscrizione o comunicazione prevista dagli artt. da 208 a 216 del medesimo decreto.

Una responsabilità del produttore dei rifiuti – come potrebbe essere la Società – potrebbe configurarsi a titolo di concorso nel reato. Ciò, non solo in caso di conoscenza della natura illecita dell'attività di gestione dei rifiuti concessa in appalto, ma anche in caso di violazione di specifici obblighi di controllo sul soggetto incaricato alla raccolta e smaltimento dei Rifiuti prodotti. Si tenga, infatti, presente che tutti i soggetti coinvolti nel complesso delle attività di gestione dei rifiuti – tra cui anche il produttore degli stessi – sono tenuti, non solo al rispetto delle disposizioni normative relative al proprio ambito di attività, ma anche ad un controllo sulla corretta esecuzione delle attività precedenti o successive alla propria. Di conseguenza, il produttore di rifiuti è tenuto a controllare che il soggetto a cui venga affidata la raccolta, il trasporto o lo smaltimento degli stessi svolga tali attività in modo lecito.

Esempio

La Banca affida il servizio di smaltimento dei propri rifiuti ad un operatore esterno, pur sapendo che questi non è un soggetto autorizzato a svolgere tale attività.

FALSITÀ NELLA PREDISPOSIZIONE DI UN CERTIFICATO DI ANALISI DEI RIFIUTI (ART. 258, CO. 4, D.LGS. 152/2006)

L'art. 258 del D.lgs. 152/2006 – rilevante ai fini del Decreto 231 nel suo solo comma 4 – sanziona la condotta di chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, nonché chi fa uso di un certificato falso durante il trasporto.

Tale disposizione va coordinata con gli artt. 190 e 193 del D.lgs. 152/2006, che individuano gli obblighi di tenuta (i) dei registri di carico e scarico e (ii) del formulario di identificazione dei rifiuti.

La fattispecie individua un reato contravvenzionale, per cui ne è possibile la commissione anche per mera colpa.

Esempio

La Banca, per risparmiare sui relativi costi, omette di effettuare i controlli sul Dipendente delegato alla sottoscrizione dei formulari di identificazione dei rifiuti, in tal modo non avvedendosi che questi effettua valutazioni scorrette sulla classificazione dei rifiuti.

TRAFFICO ILLECITO DI RIFIUTI (ART. 259, D.LGS. 152/2006)

L'art. 259, comma 1 del D.lgs. 152/2006 sanziona due diverse fattispecie connesse alla spedizione transfrontaliera di rifiuti e, in particolare, la condotta di colui che: (i) effettua – tra gli altri – una spedizione di rifiuti senza inviare la notifica o senza il consenso delle autorità competenti interessate, ovvero con il consenso delle autorità competenti interessate ottenuto mediante falsificazioni, false dichiarazioni o frode, oppure nel caso in cui la spedizione dei rifiuti non sia specificata nel documento di accompagnamento o comporti uno smaltimento o un recupero in violazione delle norme comunitarie o internazionali; (ii) effettua la spedizione di rifiuti destinati al recupero violando le regole relative all'individuazione degli impianti di destinazione e, in generale, le condizioni previste dall'art. 1 del regolamento CEE del 1 febbraio 1993, n. 259.

Anche tale fattispecie, come quella in precedenza esaminata, individua un reato contravvenzionale: ne è dunque possibile la commissione anche a titolo di colpa.

Esempio

La Banca, avendo negoziato un prezzo particolarmente vantaggioso rispetto agli standard di mercato, affida ad un operatore esterno lo smaltimento dei propri rifiuti, senza verificare il luogo di destinazione degli stessi e così ignorando, per colpa, che tale operatore li spedisce all'estero senza indicare il luogo di destinazione nei documenti di accompagnamento.

SISTEMA INFORMATICO DI CONTROLLO DELLA TRACCIABILITÀ DEI RIFIUTI (ART. 260-*BIS*, D.LGS. 152/2006)

L'art. 260-*bis,* co. 6, D.lgs. 152/2006 puniva colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti fornisse false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e chi inserisse un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti.

Tali fattispecie di reato non sono più attuali in ragione dell'avvenuta abolizione del Sistema Informatico di Controllo della Tracciabilità dei Rifiuti (c.d. SISTRI).

Esempio

La Banca, avendo negoziato un contratto particolarmente vantaggioso rispetto agli standard di mercato con una impresa trasportatrice di rifiuti che aderisce al SISTRI, ignora, per colpa, che la medesima impresa fa sistematicamente uso di certificati di analisi di rifiuti falsi.

13.2. Processi e attività sensibili rilevanti

In relazione ai Reati di cui all'art. 25-*undecies* del Decreto, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

I. Gestione degli adempimenti e dei rapporti con gli enti pubblici e le autorità amministrative indipendenti, anche in occasione di verifiche ispettive;

XIV. Gestione degli impatti ambientali generati dalle attività e dai processi.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Gestione delle attività di raccolta, deposito, trasporto e smaltimento di rifiuti prodotti nell'ambito delle attività aziendali, anche tramite l'affidamento delle attività a società terze (e.g. toner; RAEE, ecc.)

- Processo Sensibile principale: **XIV**

b) Gestione comunicazioni e adempimenti, cartacei o telematici, verso la PA connessi a gestione, anche attraverso fornitori esterni, di formulari e di certificati di analisi dei rifiuti e gestione della tenuta dei registri obbligatori in materia di tracciabilità dei rifiuti

- Processi Sensibili principali: **I** e **XIV**

13.3. Principi generali di comportamento

I principi generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali ai Fornitori e ai Consulenti della Società.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*undecies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

Al fine di presidiare i rischi di commissione di reati ambientali, in particolare, la politica aziendale in materia di tutela dell'ambiente si ispira ai seguenti principi:

- promozione tra tutti i Destinatari di un senso di responsabilità verso l'ambiente;
- generale valutazione delle potenziali ripercussioni delle attività svolte sull'ambiente locale;
- riduzione della produzione di rifiuti;
- rispetto della normativa tempo per tempo vigente.

La Banca identifica ed attua misure idonee affinché il personale, ai diversi livelli e in ragione dell'attività svolta:

- sia consapevole dell'importanza del rispetto degli obiettivi ambientali prefissati dalla Banca;
- abbia una conoscenza adeguata, ciascuno in relazione alle rispettive mansioni, della normativa rilevante in materia ambientale, anche con riferimento all'applicazione della disciplina di cui al Decreto;
- assuma un comportamento orientato alla massima collaborazione e disponibilità nel caso di ispezioni in materia ambientale effettuate dall'Autorità competente;
- non cagioni inquinamenti di sorta o non contribuisca a cagionare inquinamenti in ogni matrice ambientale.

13.4. Principi specifici per le singole attività sensibili

Con riferimento alle Attività Sensibili individuate *supra* §13.2, si applicano i seguenti principi.

a) Gestione delle attività di raccolta, deposito, trasporto e smaltimento di rifiuti prodotti nell'ambito delle attività aziendali, anche tramite l'affidamento delle attività a società terze (e.g. toner; RAEE, ecc.)

GESTIONE DEI RIFIUTI AZIENDALI NELL'AMBITO DELL'ATTIVITÀ D'UFFICIO

i La Banca definisce i principali adempimenti da porre in essere in ambito aziendale in merito alla gestione delle diverse tipologie di rifiuti prodotti dalla Banca, soprattutto in riferimento alla gestione di rifiuti speciali, quali toner e materiale elettronico e informatico;

ii La Banca provvede alla raccolta e alla classificazione dei rifiuti prodotti nell'ambito delle attività aziendali in conformità a quanto stabilito dalle disposizioni normative vigenti. Con particolare riferimento ai rifiuti elettronici e informatici: la Banca: (i) istituisce e tiene costantemente aggiornato il registro dei materiali elettronici e informatici in disuso; (ii) conserva e archivia i certificati relativi al corretto smaltimento dei rifiuti elettronici e informatici ricevuti dai fornitori dei servizi di gestione degli stessi;

iii La Banca inserisce nei contratti stipulati con i Fornitori di servizi connessi alla gestione dei rifiuti specifiche clausole attraverso le quali si riserva il diritto di verificare periodicamente le comunicazioni, certificazioni e autorizzazioni in materia ambientale, tenendo in considerazione i termini di scadenza e rinnovo delle stesse;

iv La Banca informa adeguatamente il personale dipendente in merito alla differenziazione e raccolta di rifiuti, soprattutto in relazione alla separazione e al deposito dei rifiuti speciali in appositi contenitori e/o in luoghi specificamente dedicati;

v La Banca affida le attività di trasporto, recupero e smaltimento dei rifiuti esclusivamente a imprese autorizzate e nel rispetto delle procedure aziendali relative alla selezione dei fornitori di servizi; i contratti con tali imprese devono prevedere l'impegno delle stesse a non porre in essere condotte tali da integrare i reati contemplati nel Decreto 231.

- ✓ **Control Owner:** Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

GESTIONE DELLE ATTIVITÀ DI RACCOLTA, RECUPERO, SMALTIMENTO E INTERMEDIAZIONE DI RIFIUTI ANCHE TRAMITE L'AFFIDAMENTO A SOCIETÀ TERZE

vi La Banca, nell'ambito del ricorso a Fornitori per le attività di smaltimento di rifiuti prodotti, prima dell'instaurazione del rapporto, accerta la rispettabilità e l'affidabilità anche attraverso l'acquisizione e la verifica delle comunicazioni, certificazioni e autorizzazioni in materia ambientale da questi effettuate o acquisite a norma di legge;

vii La Banca, prima dell'instaurazione del rapporto, richiede ai Fornitori di servizi connessi alla gestione dei rifiuti, ove richiesto dal D.lgs. 152/2006 e dalle ulteriori fonti normative e regolamentari, di dare evidenza, in base alla natura del servizio prestato, del rispetto della disciplina in materia di gestione dei rifiuti e di tutela dell'ambiente, secondo quanto stabilito nelle procedure aziendali;

viii La Banca, prima dell'instaurazione del rapporto, verifica il possesso da parte dei Fornitori delle autorizzazioni relative al rifiuto specifico sia con riferimento ai trasportatori, sia in relazione all'impianto di smaltimento finale;

ix La Banca garantisce la corretta gestione dei depositi temporanei dei rifiuti sulla base della tipologia e dei quantitativi di rifiuti prodotti. Il deposito temporaneo di rifiuti, deve essere implementato prevedendo: la definizione dei criteri per la scelta/realizzazione delle aree adibite al deposito temporaneo di rifiuti; l'identificazione delle aree adibite al deposito temporaneo di rifiuti; la raccolta dei rifiuti per categorie omogenee e l'identificazione delle tipologie di rifiuti ammessi all'area adibita a deposito temporaneo e l'avvio delle operazioni di recupero o smaltimento dei rifiuti raccolti, in linea con la periodicità indicata e/o al raggiungimento dei limiti quantitativi previsti dalla normativa vigente.

b) Gestione comunicazioni e adempimenti, cartacei o telematici, verso la PA connessi a gestione, anche attraverso fornitori esterni, di formulari e di certificati di analisi dei rifiuti e gestione della tenuta dei registri obbligatori in materia di tracciabilità dei rifiuti

i Gli adempimenti e la predisposizione della documentazione destinata agli enti della Pubblica Amministrazione preposti al controllo della normativa ambientale nel rispetto delle leggi vigenti, nazionali, comunitarie e internazionali, sono effettuati con la massima diligenza e professionalità, in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere;

ii L'archivio delle autorizzazioni, iscrizioni e comunicazioni acquisite dalla Società e dai fornitori terzi sono monitorate continuativamente e periodicamente aggiornate;

iii La Banca gestisce tutte le scadenze concernenti gli adempimenti in materia ambientale attraverso un software applicativo dedicato.

14. Reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare

14.1. La fattispecie di reato rilevante di cui all'art. 25-*duodecies*, D.lgs. 231/2001

ART. 22, CO. 12-*BIS*, D.LGS. 286/1998

Il reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare è punito dall'art. 22, co. 12-*bis*, D.lgs. 286/1998 e si configura qualora il soggetto che riveste la qualifica di Datore di Lavoro occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o sia stato revocato o annullato, laddove i lavoratori occupati siano:

- in numero superiore a tre;
- minori in età non lavorativa;
- sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui all'art. 603-*bis* c.p.

Esempio

La Banca assume Lavoratori di paesi terzi privi di permesso di soggiorno.

14.2. Processi e attività sensibili rilevanti

In relazione al Reato di cui all'art. 25-*duodecies* del Decreto, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

VII. Acquisto di beni, servizi e consulenze;

VIII. Selezione, assunzione e gestione del personale.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Assunzione di personale dipendente comunitario e/o extracomunitario

- Processo Sensibile principale: **VIII**

b) Gestione degli acquisti, con particolare riferimento all'affidamento di attività che prevedano l'utilizzo di manodopera di terze parti per la fornitura del personale e/o servizi (*e.g.*, appalti d'opere e di servizi)

- Processo Sensibile principale: **VII**

14.3. Principi generali di comportamento

I principi generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché ai Consulenti Finanziari della Banca.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*duodecies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

In particolare, fermi i principi generali e specifici di comportamento di cui al capitolo 7 della presente Parte Speciale, è fatto esplicito divieto di assumere Dipendenti stranieri privi di permesso di soggiorno regolare e di conferire incarichi ad appaltatori o subappaltatori che, al contrario, se ne avvalgono.

14.4. Principi specifici per le singole attività sensibili

Con riferimento alle Attività Sensibili individuate *supra* §14.2, si applicano i seguenti principi.

a) Assunzione di personale dipendente comunitario e/o extracomunitario

i In caso di assunzione di cittadini stranieri residenti in paesi extracomunitari, la Banca si attiva presso le autorità competenti al fine di ottenere tutta la documentazione necessaria a consentire l'ingresso legale in Italia del cittadino straniero e l'instaurazione dl un rapporto di lavoro regolare;

ii In caso di assunzione di cittadini stranieri già soggiornanti in Italia la Banca verifica che i medesimi siano in possesso di un permesso di soggiorno regolare o che in caso di scadenza dello stesso i medesimi abbiano provveduto ad avviare le pratiche per il rinnovo;

iii La Banca controlla che in occasione della scadenza dei permessi di soggiorno dei Dipendenti stranieri, questi ultimi abbiamo provveduto ad avviare le relative pratiche di rinnovo, assicurando loro collaborazione nel rilascio della documentazione attestante l'impiego regolare presso la Banca.

iv La Banca assicura che, qualora l'adempimento delle attività descritte ai punti precedenti avvenisse ricorrendo ai servizi di un'agenzia esterna specializzata, il rapporto con quest'ultima sia disciplinato da accordo scritto, il quale preveda l'obbligo dell'agenzia esterna a non porre in essere comportamenti che violino le disposizioni di cui al Decreto 231 e a rispettare per quanto applicabile il Modello della Banca.

- ✓ ***Control Owner*:** Unità Organizzativa Consulenza Legale Banca; Responsabile Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica; Procedura Selezione e valutazione del personale e politiche retributive; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa; Funzionigramma

b) Gestione degli acquisti, con particolare riferimento all'affidamento di attività che prevendano l'utilizzo di manodopera di terze parti per la fornitura del personale e/o servizi (*e.g.*, appalti d'opere e di servizi)

i La Banca si assicura che nei contratti di appalto sia inserito l'impegno da parte dell'appaltatore ad ottemperare a tutti gli obblighi verso i dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro ed assicurazioni sociali, assumendo a suo carico tutti gli oneri relativi;

ii La Banca si assicura che nei contratti di appalto sia inserita la garanzia da parte dell'appaltatore di impiegare nella prestazione di servizi a favore della Banca esclusivamente lavoratori stranieri lecitamente soggiornanti in Italia e con rapporto di lavoro regolare;

iii La Banca si assicura che nei contratti di appalto sia inserito l'obbligo dell'appaltatore a non porre in essere comportamenti che violino le disposizioni di cui al Decreto 231 e a rispettare per quanto applicabile il Modello;

iv La Banca si assicura che nei contratti di appalto sia inserita la facoltà da parte della Banca di richiedere in ogni momento tutta la documentazione utile a verificare l'origine, le condizioni e il trattamento della forza lavoro.

- ✓ ***Control Owner*:** Unità Organizzativa Consulenza Legale Banca; Responsabile Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione della contrattualistica

15. Reati tributari

15.1. Le fattispecie di reato rilevanti di cui all'art. 25-*quinquiesdecies*, D.lgs. 231/2001

La legge 19 dicembre 2019, n. 157, di conversione del decreto legge 26 ottobre 2019, n. 124 (c.d. "Decreto Fiscale"), ha previsto l'inserimento nel catalogo dei Reati Presupposto del Decreto (in particolare, all'art. 25-*quinquiesdecies*) anche di taluni reati fiscali regolati dal decreto legislativo 10 marzo 2000, n. 74.

Si tratta, nello specifico, dei delitti di (**i**) dichiarazione fraudolenta mediante uso di fatture false o altri documenti per operazioni inesistenti (art. 2, D.lgs. 74/2000); (**ii**) dichiarazione fraudolenta mediante altri artifici (art. 3, D.lgs. 74/2000); (**iii**) emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.lgs. 74/2000); (**iv**) occultamento o distruzione di documenti contabili (art. 10, D.lgs. 74/2000); e (**v**) sottrazione fraudolenta al pagamento delle imposte (art. 11, D.lgs. 74/2000).

L'art. 25-*quinquiesdecies* del Decreto è stato, dopo qualche mese, nuovamente oggetto di integrazione, poiché, in sede di attuazione della direttiva (UE) 2017/1317 relativa alla lotta contro le frodi che ledono gli interessi finanziari dell'Unione mediante il diritto penale, con il decreto legislativo 14 luglio 2020, n. 75, il legislatore italiano ha aggiunto anche le seguenti fattispecie (**vi**) dichiarazione infedele (art. 4, D.lgs. 74/2000); (**vii**) omessa dichiarazione (art. 5, D.lgs. 74/2000); e (**viii**) indebita compensazione (art. 10-*quater*, D.lgs. 74/2000). Tuttavia, seguendo gli obblighi imposti dall'Unione europea nella direttiva sopra menzionata, il legislatore italiano ha ristretto l'ambito di applicazione della responsabilità da reato degli enti per questi ultimi tre reati solo ove gli stessi siano «*commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo non inferiore a dieci milioni di euro*». Per tale ragione, a seguito del *risk assessment* condotto anche con il supporto di Consulenti esterni, la Banca, in considerazione del proprio *core business*, ha ritenuto non astrattamente rilevanti queste fattispecie.

DICHIARAZIONE FRAUDOLENTA MEDIANTE USO DI FATTURE FALSE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 2, D.LGS. 74/2000)

Tale reato sanziona la condotta di chi, al fine di evadere le imposte sui redditi (ad esempio, l'IRES) o l'IVA, avvalendosi di fatture o altri documenti per operazioni inesistenti (come, p.e., scontrini, schede carburante, bolle di accompagnamento, documenti di trasporto, note di addebito/credito, ecc.), indica in una delle dichiarazioni relative a tali imposte elementi passivi fittizi, quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti per fini probatori nei confronti dell'amministrazione finanziaria.

La pena detentiva e, corrispondentemente, la sanzione pecuniaria prevista dall'art. 25-*quinquiesdecies* del Decreto è però attenuata se l'ammontare degli elementi passivi fittizi è inferiore a 100.000 euro.

L'offesa del reato consiste nella rappresentazione mendace della propria situazione reddituale, accompagnata da una condotta costituita dall'utilizzo di falsi documenti probatori, che rende assai più arduo per l'amministrazione finanziaria ricostruire la reale posizione del contribuente.

Il reato fa riferimento a qualsiasi dichiarazione fiscale – quindi non soltanto alla dichiarazione annuale dei redditi – e sanziona soltanto l'indicazione in essa di valori negativi che determinano o una base imponibile inferiore rispetto a quella effettiva (ad esempio, per effetto dell'incremento fraudolento dei costi sostenuti per generare il reddito) o un'imposta più bassa rispetto a quella invece dovuta (ad esempio, per effetto del calcolo di detrazioni indebite).

Quanto alle operazioni che, richiamate dalle fatture, devono risultare inesistenti, il reato sussiste sia nel caso di inesistenza totale dell'operazione economica, sia nel caso di inesistenza parziale (ad esempio, una compravendita di beni per un ammontare inferiore a quello indicato in fattura); l'inesistenza dell'operazione, poi, può essere sia *oggettiva* – laddove, cioè, la prestazione indicata in fattura non sia mai stata effettuata o lo sia stata in maniera diversa da come rappresentato – sia *soggettiva* – laddove, cioè, la prestazione, pur effettivamente avvenuta, sia intercorsa tra soggetti diversi da quelli indicati in fattura.

Il reato in esame, da ultimo, è punito soltanto a titolo doloso.

Esempio

La Banca indica nella dichiarazione annuale dei redditi taluni costi per iniziative di marketing "gonfiati" dall'agenzia pubblicitaria, che ne ha retrocesso una parte ad un esponente aziendale e, come tali, documentati da false fatture.

DICHIARAZIONE FRAUDOLENTA MEDIANTE ALTRI ARTIFICI (ART. 3, D.LGS. 74/2000)

Tale reato rappresenta un'ipotesi residuale rispetto a quella disciplinata dall'art. 2 appena richiamata, perché qui la condotta sanzionata non è costituita dall'utilizzo di fatture false, ma dall'avere – alternativamente – realizzato operazioni simulate soggettivamente o oggettivamente, dall'essersi avvalsi di documenti falsi (ad esempio, fatture contraffatte) o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, con la finalità di evadere le imposte sui redditi o sul valore aggiunto.

Peraltro, è sanzionata sia la condotta di indicazione nella dichiarazione di elementi attivi per un ammontare inferiore a quello effettivo, sia di elementi passivi, crediti e ritenute fittizi. Diversamente dalla fattispecie di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, nel delitto in esame è prevista una duplice soglia di punibilità. In particolare (**a**) l'imposta evasa deve essere superiore, con riferimento alle singole imposte, a € 30.000; e (**b**) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, deve essere superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, deve essere superiore a € 1.500.000, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta è superiore al 5% dell'ammontare dell'imposta medesima o comunque a € 30.000.

Come per l'art. 2 del D.lgs. 74/2000, anche per la dichiarazione fraudolenta mediante altri artifici il fatto si considera commesso «*avvalendosi di documenti falsi*» quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Per un corretto inquadramento del reato, si deve segnalare che la legge qualifica come «*operazioni simulate oggettivamente o soggettivamente*» le operazioni apparenti, diverse da quelle che si concretizzano in fatti di elusione fiscale (cioè nel ricorso a fatti, atti e contratti che, pur nel rispetto formale delle norme fiscali, hanno il solo scopo di realizzare un vantaggio fiscale indebito quale effetto dell'operazione), poste in essere senza la volontà di realizzarle effettivamente, ovvero che sono riferite a soggetti fittiziamente interposti.

La legge, poi, offre alcuni riferimenti per la definizione dei «*mezzi fraudolenti*»: in positivo, si tratta di condotte artificiose attive o omissive, realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà; in negativo, non sono rappresentati dalla semplice violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o dalla sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali. In breve, la semplice sotto-fatturazione (il c.d. nero) non ricade nell'ipotesi in esame.

Anche in questo caso, il reato è punito soltanto a titolo doloso.

Esempio

La Banca indica nella dichiarazione annuale dei redditi un ammontare dei ricavi per le vendite in misura inferiore al reale, predisponendo, per ostacolare l'accertamento, un documento falso.

EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 8, D.LGS. 74/2000)

La fattispecie di reato si realizza allorché un soggetto, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Ai fini di quanto sopra indicato, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica per la persona fisica – e per la persona giuridica – una pena attenuata.

Esempio

La Banca emette delle false fatture al fine di consentire a terzi un indebito e fraudolento abbassamento dell'imponibile fiscale, relativo alle imposte sui redditi o sul valore aggiunto.

OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART. 10, D.LGS. 74/2000)

Tale fattispecie punisce, salvo che il fatto costituisca più grave reato, chiunque, al fine di evadere le imposte sui redditi (come, p.e., l'IRES) o l'imposta sul valore aggiunto, ovvero al fine di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume d'affare.

Tale condotta, pertanto, consiste nell'indisponibilità della documentazione da parte degli stessi organi verificatori, sia essa temporanea o definitiva. Il reato è integrato in tutti i casi in cui la distruzione o l'occultamento della documentazione contabile dell'impresa non consenta o renda difficoltosa la ricostruzione delle operazioni.

Esempio

Un Dipendente della Banca, al fine di consentire alla stessa di versare una somma inferiore di IRES rispetto a quanto effettivamente dovuto dalla Società, distrugge parte delle scritture contabili della Banca.

SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DELLE IMPOSTE (ART. 11, D.LGS. 74/2000)

Il reato di sottrazione fraudolenta al pagamento delle imposte, disciplina due distinte ipotesi.

In particolare, il primo comma dell'art. 11 D.lgs. 74/2000 punisce chiunque al fine di sottrarsi al pagamento delle imposte sui redditi o sul valore aggiungo – ovvero dei rispettivi interessi o sanzioni amministrative – di ammontare superiore a € 50.000, *aliena simulatamente* o compie altri *atti fraudolenti* sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. La pena è aumentata se l'ammontare di imposte, sanzioni e interesse è superiore a € 200.000.

Inoltre, ai sensi del secondo comma, l'art. 11 D.lgs. 74/2000 punisce chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi per un ammontare complessivo superiore a € 50.000 (se l'ammontare è superiore a € 200.000, la pena è aumentata).

Esempio

La Banca, nell'ambito di una transazione fiscale con l'amministrazione finanziaria, indica nella documentazione presentata elementi attivi per un ammontare inferiore a quello effettivo.

15.2. Processi e attività sensibili rilevanti

In relazione ai Reati tributari di cui all'art. 25-*quinquiesdecies* del Decreto, i Processi Sensibili della Banca potenzialmente più esposti al rischio di commissione di illeciti sono i seguenti:

- **II.** Gestione dei flussi monetari e finanziari;
- **III.** Selezione e gestione dei promotori finanziari;
- **IV.** Formazione del bilancio e gestione degli adempimenti e dei rapporti con gli organi di controllo;
- **V.** Commercializzazione dei prodotti bancari, finanziari e assicurativi;
- **VII.** Acquisto di beni, servizi e consulenze;
- **XVII.** Gestione della fiscalità aziendale.

Nello specifico, all'interno dei singoli Processi Sensibili, sono state individuate le seguenti Attività Sensibili:

a) Acquisto di beni, servizi e consulenze

- Processi Sensibili principali: **II** e **VII**

b) Selezione e gestione delle controparti contrattuali, con particolare riferimento ai consulenti finanziari abilitati all'offerta fuori sede

- Processo Sensibile principale: **III**

c) Commercializzazione dei prodotti bancari, finanziari e assicurativi, nonché servizi fiduciari

- Processo Sensibile principale: **V**

d) Gestione della contabilità generale

- Processo Sensibile principale: **IV**

e) Gestione dei rapporti e delle operazioni infragruppo

- Processo Sensibile principale: **XVII**

f) Gestione della fiscalità aziendale

- Processo Sensibile principale: **XVII**

15.3. Principi generali di comportamento

I principi generali di comportamento si applicano in via diretta a tutti i Dipendenti, Dirigenti e membri degli Organi sociali della Banca, nonché, per il tramite di apposite clausole contrattuali ai Fornitori e ai Consulenti Finanziari della Banca.

A tutti i soggetti sopra menzionati è **fatto esplicito divieto** di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino le fattispecie di reato contemplate nell'art. 25-*quinquiesdecies* del Decreto e di violare i principi e le procedure aziendali richiamate nel presente capitolo della Parte Speciale.

Inoltre tutti i Destinatari del presente Modello che, in ragione del proprio incarico o della propria funzione, sono coinvolti nelle attività relative al calcolo delle imposte e alla presentazione delle dichiarazioni fiscali, nelle attività attinenti alla gestione del ciclo attivo, del ciclo passivo e nelle attività di finanza e tesoreria **devono**:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate al calcolo delle imposte e alla presentazione delle dichiarazioni fiscali, alla formazione del bilancio, alla gestione del ciclo attivo, del ciclo passivo e a quelle di finanza e tesoreria;
- osservare rigorosamente tutte le norme poste dalla normativa fiscale e, in particolare, provvedere al puntuale e corretto adempimento degli obblighi fiscali gravanti sulla Banca;
- fornire ai Consulenti fiscali della Banca tutta la documentazione contabile relativa all'attività della Banca;
- informare l'Organismo in caso di profili di anomalia nei rapporti finanziari economici della Banca;
- con riferimento alla gestione finanziaria, assicurare la tracciabilità di tutte le operazioni monetarie, provvedendo altresì allo svolgimento dei controlli necessari a garantire la trasparenza dei flussi finanziari.

È inoltre fatto specifico **divieto** di:

- apportare modifiche ai documenti archiviati, in modo da ostacolare la tracciabilità delle decisioni assunte e dei procedimenti seguiti;
- registrare nelle scritture contabili obbligatorie documenti falsi;
- detenere ai fini di prova nei confronti dell'amministrazione finanziaria documenti falsi;
- omettere di presentare le dichiarazioni fiscali della Banca;
- occultare o distruggere le scritture contabili o i documenti di cui è obbligatoria la conservazione;
- alienare simulatamente o compiere altri atti fraudolenti su beni della Banca idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva di eventuali debiti tributari della stessa.

15.4. Principi specifici per le singole attività sensibili

Con riferimento alle Attività Sensibili individuate *supra* §15.2, si applicano i seguenti principi.

a) Acquisto di beni, servizi e consulenze

Si rinvia a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. g) della Parte Speciale).

b) Selezione e gestione delle controparti contrattuali, con particolare riferimento ai consulenti finanziari abilitati all'offerta fuori sede

i In aggiunta a quanto previsto nel capitolo relativo ai Reati nei rapporti con la PA (§1.5, lett. l) della Parte Speciale), a cui si rinvia integralmente, la Banca adotta una specifica *policy* aziendale che prevede che: (i) le incentivazioni ai Consulenti Finanziari abilitati all'offerta fuori sede siano riconosciute a fronte di comprovate ragioni che ne giustifichino, a seguito di dettagliata e collegiale valutazione, la dazione; (ii) la tracciatura del processo autorizzativo di concessione delle incentivazioni ai Consulenti Finanziari abilitati all'offerta fuori sede.

- ✓ ***Control Owner***: Direzione Commerciale; Unità Organizzativa Incentivi (per la definizione degli obiettivi ROR/SII, principali sistemi di incentivazione della Rete dei PFD e dei PFA); Unità Organizzativa Controlli Banca (per la valutazione degli *inducement* identificati come *proper fee)*
- ✓ ***Documentazione interna di riferimento***: Procedura Gestione delle incentivazioni ai Consulenti finanziari abilitati all'offerta fuori sede; Procedura Gestione degli incentivi; Policy Gestione degli incentivi; Procedura Gestione del Piano di incentivazione di Soggetti Rilevanti

c) Commercializzazione dei prodotti bancari, finanziari e assicurativi, nonché servizi fiduciari

i La Banca prevede condizioni contrattuali standardizzate relative ai prodotti collocati, non modificabili in senso peggiorativo per il cliente finale;

- ✓ ***Control Owner***: Unità Organizzativa Legale
- ✓ ***Documentazione interna di riferimento***: Gestione della contrattualistica

ii La Banca adotta un modello di remunerazione dei Consulenti Finanziari abilitati all'offerta fuori sede e delle figure interne alla Banca responsabili delle aree di business in esame, tale da disincentivare condotte corruttive;

- ✓ ***Control Owner***: Responsabile della Direzione Risorse (per le strategie definite nell'ambito del processo di *Strategic Dialogue* e del *budget*)
- ✓ ***Documentazione interna di riferimento***: Gestione delle incentivazioni ai Consulenti finanziari abilitati all'offerta fuori sede

iii La Banca effettua costanti controlli *ex post* sulla rete dei Consulenti Finanziari abilitati all'offerta fuori sede al fine di verificare l'eventuale collocamento di prodotti non nell'interesse del cliente finale;

- ✓ ***Control Owner*:** Unità Organizzativa Analisti Rete; Unità Organizzativa Ispettori Rete
- ✓ ***Documentazione interna di riferimento***: Procedura Controlli sulla rete dei Consulenti finanziari abilitati all'offerta fuori sede

d) Gestione della contabilità generale

i L'Unità Organizzativa Amministrazione custodisce in modo corretto e ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e informatiche che impediscano eventuali atti di distruzione o occultamento;

ii La Banca assicura che sia attuato il coordinamento tra le funzioni coinvolte nella redazione delle suddette scritture interne all'Ufficio coinvolte, nonché tra le eventuali ulteriori funzioni aziendali che prendono parte al relativo *iter*;

- ✓ ***Control Owner*:** Unità Organizzativa Amministrazione; Unità Organizzativa Contabilità e Bilancio
- ✓ ***Documentazione interna di riferimento***: Procedura Tenuta della contabilità generale; Procedura Tenuta dei libri contabili obbligatori; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa; Funzionigramma; Procedura Predisposizione situazioni periodiche; Procedura Redazione del bilancio annuale individuale e consolidato

iii L'Unità Organizzativa Amministrazione prevede un controllo finale di tipo "operativo" che consenta di accertare la veridicità e la completezza dei dati riflessi nelle dichiarazioni di natura contabile e nei dati e nelle informazioni contabili;

iv La Banca attua un attento monitoraggio del rispetto dei principi che regolano la compilazione, tenuta e conservazione dei dati e delle informazioni contabili delle dichiarazioni di natura contabile dei dati e delle informazioni contabili;

- ✓ ***Control Owner*:** Unità Organizzativa Amministrazione - Unità Organizzativa Vigilanza e Reporting
- ✓ ***Documentazione interna di riferimento***: Procedura Tenuta della contabilità generale; Procedura Tenuta dei libri contabili obbligatori; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa; Funzionigramma; Procedura Predisposizione situazioni periodiche; Procedura Redazione del bilancio annuale individuale e consolidato

v La Banca garantisce l'apposizione di adeguate difese fisiche e/o informatiche a protezione dei luoghi in cui sono custodite le scritture contabili in moda da impedire eventuali atti di distruzione e/o occultamento;

- ✓ ***Control Owner*:** Unità Organizzativa Amministrazione - Unità Organizzativa Contabilità e Bilancio
- ✓ ***Documentazione interna di riferimento***: Procedura Tenuta dei libri contabili obbligatori

vi La Banca identifica i soggetti autorizzati all'apertura dei conti correnti societari e definisce le modalità di gestione dei conti correnti societari;

vii È assicurato il rispetto della segregazione dei ruoli tra chi gestisce i conti correnti, chi effettua le riconciliazioni bancarie e chi le approva.

- ✓ ***Control Owner*:** Unità Organizzativa Amministrazione - Unità Organizzativa Gestione Conto
- ✓ ***Documentazione interna di riferimento***: Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa; Funzionigramma

e) Gestione dei rapporti e delle operazioni infragruppo

i La Società prevede la proceduralizzazione delle singole fasi di emissione delle fatture infragruppo e l'interazione tra le diverse figure aziendali che prendono parte a tale attività ed effettuano un controllo sistematico dell'effettivo espletamento da parte della Società dell'attività per cui viene emessa relativa fattura o dell'effettivo espletamento dell'attività per cui, a fronte del ricevimento della fattura, la Società effettua il pagamento.

f) Gestione della fiscalità aziendale

i Prima di effettuare pagamenti relativi ad acquisti di beni o servizi la Società verifica l'avvenuta prestazione del servizio o la ricezione del bene. Sono definite e formalizzate le attività di verifica dell'allineamento tra l'entrata merce o l'avvenuta prestazione del servizio, il relativo ordine d'acquisto e la fattura ricevuta dal Fornitore;

ii La Banca, nella predisposizione delle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto, anche in relazione alle attività svolte per le altre società del Gruppo, si dota di presidi tali che gli esponenti aziendali coinvolti, nell'ambito delle rispettive competenze: (a) non indichino elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti; (b) non indichino elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;

- ✓ ***Control Owner*:** Unità Organizzativa Amministrazione - Unità Organizzativa Fiscale
- ✓ ***Documentazione interna di riferimento***: Proceduta Tenuta della contabilità in outsourcing; Procedura Gestione fiscalità Banca – imposte dirette e indirette; Procedura Presidio Specialistico di Compliance – Fiscale; Procedura tenuta della contabilità generale; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Gestione fiscalità Banca – Sostituto d'Imposta; Procedura Gestione del ciclo passivo

iii La Banca si dota di presidi tali che gli esponenti aziendali coinvolti nell'ambito delle rispettive competenze non indichino una base imponibile in misura inferiore a quella effettiva attraverso l'esposizione di elementi attivi per un ammontare inferiore a quello reale o di elementi passivi fittizi;

iv La Banca si dota di presidi tali che gli esponenti aziendali coinvolti - nell'ambito delle rispettive competenze: non facciano decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle medesime così come per il successivo versamento delle imposte da esse risultanti.

- ✓ ***Control Owner*:** Unità Organizzativa Amministrazione - Unità Organizzativa Fiscale
- ✓ **Documentazione interna di riferimento**: Procedura Tenuta della contabilità in outsourcing; Procedura Gestione fiscalità Banca – imposte dirette e indirette; Procedura Presidio Specialistico di Compliance – Fiscale; Procedura tenuta della contabilità generale; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Gestione fiscalità Banca – Sostituto d'Imposta

v La Banca provvede poi a comunicare, con periodicità mensile, alla Capogruppo Allianz SE il bilancio individuale redatto secondo i principi contabili internazionali e in conformità con le indicazioni ricevute direttamente da Allianz SE;

vi La Società prevede un controllo finale di tipo "operativo" che consenta di accertare la veridicità e la completezza dei dati riflessi nei dati e nelle informazioni contabili.

- ✓ ***Control Owner*:** Unità Organizzativa Amministrazione - Unità Organizzativa Vigilanza e Reporting
- ✓ ***Documentazione interna di riferimento***: Proceduta Tenuta della contabilità in outsourcing; Procedura Gestione fiscalità Banca – imposte dirette e indirette; Procedura Presidio Specialistico di Compliance – Fiscale; Procedura tenuta della contabilità generale; Regolamento interno per l'ordinamento e il funzionamento della struttura

organizzativa – Funzionigramma; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Gestione fiscalità Banca – Sostituto d'Imposta

vii La Società, anche attraverso la predisposizione di specifiche procedure, si impegna a garantire l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione delle contabilità aziendale e nella successiva trasposizione nelle dichiarazioni tributarie con riferimento, a titolo esemplificativo, a: controllo sull'effettività delle prestazioni rispetto alle fatture emesse; verifica della veridicità delle dichiarazioni rispetto alle scritture contabili.

- ✓ ***Control Owner*****:** Unità Organizzativa Amministrazione - Unità Organizzativa Contabilità e Bilancio ed Unità Organizzativa Fiscale
- ✓ ***Documentazione interna di riferimento***: Proceduta Tenuta della contabilità in outsourcing; Procedura Gestione fiscalità Banca – imposte dirette e indirette; Procedura Presidio Specialistico di Compliance – Fiscale; Procedura tenuta della contabilità generale; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Gestione fiscalità Banca – Sostituto d'Imposta

viii La Banca identifica i ruoli e le responsabilità relativi alla gestione della fiscalità;

ix La Banca prevede attività di controllo e monitoraggio nell'ambito delle attività di predisposizione, verifica e trasmissione di dichiarazioni e comunicazioni fiscali (con riferimento sia alle dichiarazioni annuali / periodiche che alle dichiarazioni conseguenti alla messa in liquidazione, alle dichiarazioni nell'ipotesi di trasformazione, fusione e scissione societaria, alle dichiarazioni di operazioni intracomunitarie relative agli acquisti, etc.);

x La Banca prevede interventi periodici di aggiornamento e formazione indirizzati alle strutture organizzative che intervengono nel processo di gestione della fiscalità.

- ✓ ***Control Owner*****:** Unità Organizzativa Amministrazione - Unità Organizzativa Contabilità e Bilancio ed Unità Organizzativa Fiscale
- ✓ ***Documentazione interna di riferimento***: Proceduta Tenuta della contabilità in outsourcing; Procedura Gestione fiscalità Banca – imposte dirette e indirette; Procedura Presidio Specialistico di Compliance – Fiscale; Procedura tenuta della contabilità generale; Regolamento interno per l'ordinamento e il funzionamento della struttura organizzativa – Funzionigramma; Procedura Redazione del bilancio annuale individuale e consolidato; Procedura Gestione fiscalità Banca – Sostituto d'Imposta

allianzbank.it