MODELLO DI ORGANIZZAZIONE E GESTIONE

AI SENSI DEL D. LGS. 231/01

Sommario

PREMESSA

PARTE I - Parte Generale

1. Il Decreto Legislativo 231/2001

Opel Bank succursale italiana di Opel Bank S.A. (di seguito la Società o Opel Bank Italia) ha adottato il presente Modello aggiornato a seguito della trasformazione in succursale italiana di Banca estera, avvenuta a seguito di un'operazione di fusione per incorporazione (la "Fusione") di Opel Finance S.p.a., nella società di diritto francese Opel Bank S.A., la quale ha quindi costituito una succursale italiana per continuare ad operare in Italia.

Malgrado la Società non sia dotata di un'autonoma personalità giuridica, ha comunque scelto di mantenere il Modello di Organizzazione Gestione e Controllo ai sensi del D. Lgs 231/01, tenendo conto dei seguenti elementi:

- Il rapporto sussistente tra i costi marginali derivanti dal mantenimento del modello organizzativo e i benefici rilevanti;
- le eventuali conseguenze che la mancata adozione di un Modello Idoneo potrebbe produrre a carico dell'ente in caso di suo coinvolgimento nel procedimento per responsabilità amministrativa da reato (sanzioni pecuniarie, interdittive, effetti sull'immagine, sulla credibilità, etc.);
- la circostanza che l'adozione del Modello di Organizzazione e Gestione rappresenta un'esigenza imprescindibile per gli enti operanti in Italia, se non anche un vero e proprio obbligo, tanto che anche il legislatore si è orientato in tal senso presentando una proposta per rendere obbligatorio il Modello almeno per le organizzazioni di una certa entità;
- l'attività svolta dalla Società in quanto ente operante nel settore bancario.

In conformità a quanto previsto all'art. 6 lettera b) del medesimo decreto, la Società attuerà un programma di formazione rivolto a tutti i dipendenti, al fine di illustrare i rischi reato rilevati, i protocolli previsti per la prevenzione degli stessi e i comportamenti sanzionabili. La formazione sarà diversificata tra i soggetti che rivestono posizioni apicali e gli altri dipendenti.

Il presente Modello è costituito dall'insieme di principi, regole e disposizioni relativi alla gestione ed al controllo dell'attività sociale e strumentale e alla realizzazione e alla diligente gestione di un sistema di controllo delle attività sensibili finalizzato a prevenire la commissione o la tentata commissione dei reati previsti dal D.lgs. 231/2001.

Il Modello è strutturato nelle seguenti parti:

- PARTE GENERALE, che richiama i contenuti principali del decreto 231/01

- ORGANISMO DI VIGILANZA, che descrive poteri, responsabilità e modalità operative dell'organismo deputato alla verifica dell'efficacia e funzionamento del Modello ai sensi dell'art. 6 del decreto 231/01.
- GOVERNANCE ORGANIZZATIVA che descrive il sistema dei poteri interno e delle deleghe in atto, nonché il quadro normativo di riferimento entro il quale Opel Bank Italia svolge le proprie attività
- PARTE SPECIALE suddivisa in Sezioni, ciascuna delle quali è dedicata alle fattispecie di reato configurabili nella realtà societaria.

Costituiscono parte integrante del presente Modello:

- il Codice Etico
- il Sistema Disciplinare
- la Mappatura dei rischi
- il Catalogo dei reati
- le procedure aziendali che estendono la loro valenza anche alla prevenzione dei reati 231/01.

1.1 La responsabilità amministrativa degli Enti

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 – il Decreto Legislativo n. 231 recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (di seguito denominato il "Decreto"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche alle seguenti Convenzioni internazionali:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Con il Decreto è stato introdotto nel nostro ordinamento il peculiare regime di responsabilità amministrativa a carico di persone giuridiche, società e associazioni (di seguito, congiuntamente "Enti"), che è assimilabile alla responsabilità penale, per alcuni reati commessi, nell'interesse o vantaggio degli stessi da:

a) persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa, dotata di autonomia finanziaria e funzionale,

b) persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi;
c) persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità amministrativa degli Enti si aggiunge a quella della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. La responsabilità dell'Ente permane anche nel caso in cui l'autore del reato non sia identificato o non risulti punibile.

La responsabilità amministrativa degli Enti introdotta dal Decreto ha quindi comportato un radicale capovolgimento del principio tradizionalmente riconosciuto nel nostro ordinamento in virtù del quale "*societas delinquere non potest*".

1.2 I reati

Il Decreto è stato modificato più volte al fine di ampliare il catalogo dei reati dai quali può conseguire la responsabilità amministrativa dell'Ente.

1.3 Le sanzioni

Il sistema sanzionatorio contenuto nel Decreto prevede l'applicazione di:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

La sanzione pecuniaria è ridotta nel caso in cui:

a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;

b) il danno patrimoniale cagionato è di particolare tenuità, o se, prima della dichiarazione di apertura del dibattimento in primo grado:

1) l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso e

2) un Modello è stato adottato e reso operativo.

Le sanzioni interdittive si applicano in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni:

a) l'Ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti che ricoprono una posizione di rappresentanza, amministrativa o gestoria nell'Ente ovvero da soggetti sottoposti alla direzione o al controllo dei primi e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; o

b) in caso di reiterazione degli illeciti.

Le sanzioni interdittive, che possono avere una durata non inferiore a tre mesi e non superiore a due anni sono:

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

Il Decreto prevede che, qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione interdittiva, possa disporre la prosecuzione dell'attività da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, laddove ricorrano almeno una delle seguenti condizioni:

a) la società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
b) l'interruzione dell'attività può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Le misure interdittive sono applicabili anche in via cautelare - ove sussistano gravi indizi di colpevolezza dell'ente e il pericolo di reiterazione del reato - sin dalla fase delle indagini preliminari.

1.4 Condizione esimente della responsabilità amministrativa

Gli artt. 6 e 7 del Decreto prevedono forme specifiche di esonero dalla responsabilità amministrativa dell'Ente per i reati commessi nell'interesse o a vantaggio dell'Ente sia da soggetti apicali sia da dipendenti.

In particolare, nel caso di reati commessi da soggetti in posizione apicale, l'art. 6 prevede l'esonero qualora l'Ente dimostri che:

1) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione e di gestione idoneo a prevenire reati della specie di quello verificatosi;

2) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato a un Organismo dell'Ente (Organismo di Vigilanza o OdV) dotato di autonomi poteri di iniziativa e controllo;

3) le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il suddetto Modello;

4) non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV.

Nel caso di reati commessi da soggetti sottoposti alla direzione e vigilanza dei soggetti apicali, l'art. 7 prevede che l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. In ogni caso è esclusa l'inosservanza degli obblighi di direzione e vigilanza se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto prevede che il Modello debba rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi reati;

b) prevedere specifici "protocolli" diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;

c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;

d) prevedere obblighi di informazione nei confronti dell'OdV;

e) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sull'idoneità del Modello a prevenire i reati.

È infine previsto che, negli Enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente.

Con riferimento all'effettiva applicazione del Modello, il Decreto richiede:

a) una verifica periodica, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal Modello o intervengano mutamenti nell'organizzazione o nell'attività dell'Ente ovvero modifiche legislative, la modifica del Modello;
b) l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal Modello.

1.5. I reati commessi in Italia da un ente straniero

Il D.Lgs. 231/2001 non prevede specifiche disposizioni in merito alla configurazione della responsabilità amministrativa nei confronti di enti stranieri, tuttavia si evidenzia che tanto alcune pronunce giurisprudenziali quanto autorevole dottrina hanno affermato che ai fini della perseguibilità del reato presupposto ai sensi del D.Lgs. 231/2001, debba farsi riferimento al luogo di commissione dello stesso (Trib. Milano 27/04/2004 e Trib. Milano 13/06/2007).

Peraltro, secondo la medesima concezione, i reati commessi in Italia da succursali di enti stranieri o dagli enti stranieri stessi in regime di libera prestazione di servizi, determinerebbero altresì l'estensione della responsabilità amministrativa ex D.Lgs. 231/2001 in capo alla persona giuridica nell'interesse della quale è stato compiuto il reato, indipendentemente dalla sua cittadinanza.

Secondo tale orientamento, dunque, sia le persone fisiche che le persone giuridiche straniere - nel momento in cui operano in Italia - hanno semplicemente il dovere di osservare e rispettare la legge italiana e quindi anche il d.lgs. n . 231/2001.

A tal proposito, è opportuno richiamare altresí il dettato normativo dell'art. 36, co. 1 del D.lgs. 231/01 il quale, nel disciplinare la competenza giurisdizionale, non fa alcun riferimento alla sede formale dell'ente nel cui interesse o vantaggio è stato commesso il reato presupposto, ma solo al luogo in cui si è verificato il delitto.

Del resto, a conferma di quanto appena detto, da un'attenta lettura dell'art 1 del Decreto emerge chiaramente come non vi sia nessuna espressa esclusione dell'ente straniero dall'ambito di applicazione soggettivo della normativa. Parimenti, si segnala che il legislatore non opera alcuna distinzione tra ente italiano ed ente straniero, al contrario di quanto avviene per lo Stato e gli enti pubblici o aventi rilevanza costituzionali, per i quali invece vi è un'espressa preclusione.

La *ratio* di tale scelta da parte del legislatore deve certamente rinvenirsi nella necessità che l'ente straniero operante in Italia debba attivarsi per uniformarsi alla normativa nazionale vigente a prescindere dal luogo ove formalmente è collocata la sede principale, come ribadito nella già citata pronuncia del 27 aprile 2004 del Gip del Tribunale Milano :"*sia le persone fisiche che le persone giuridiche straniere nel momento in cui operano in Italia (…) hanno semplicemente il dovere di osservare e rispettare la legge italiana e quindi anche il d.lgs. n . 231/2001, indipendentemente dall'esistenza o meno nel Paese di appartenenza di norme che regolino in modo analogo la medesima materia".*

Ragionando diversamente l'ente straniero si attribuirebbe una sorta di "auto esenzione" dalla disciplina della responsabilità amministrativa, in contrasto, tra l'altro, con i principi generali di tendenziale universalità e di ubiquità della norma penale, di cui agli artt. 3 e 6 c.p., come affermato anche dall'Associazione Bancaria italiana (ABI).

Ciò premesso circa l'applicabilià della normativa di riferimento alle succursali di enti stranieri, si rende opportuna l'adozione del presente Modello di Organizzazione e Gestione aggiornato, affinchè la Società possa godere dell'esimente prevista dall'art. 6 del D.lgs. 231/2001.

1.5 Finalità del Modello 231

La Società è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine, delle aspettative dei propri azionisti e del proprio gruppo di appartenenza, e a tutela dei dipendenti; è

inoltre consapevole dell'importanza di dotarsi di un sistema di controllo interno aggiornato e idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri rappresentanti, dipendenti, e partner d'affari.

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

Con il Modello la Società intende censurare ogni comportamento illecito attraverso:

(i) la costante attività dell'Organismo di Vigilanza sull'operato delle persone rispetto ai processi sensibili individuati

(ii) la comminazione di sanzioni disciplinari o contrattuali in caso di violazioni dei principi e delle regole sanciti nel Codice Etico e nel presente Modello da parte di dipendenti o di soggetti terzi con cui la Società intrattiene rapporti nell'ambito delle Aree di attività a rischio o dei Processi strumentali/funzionali.

1.6 Destinatari

Le regole contenute nel Modello si applicano:

- a coloro i quali siano titolari, all'interno della Società, di qualifiche formali, come quelle di rappresentante legale e/o di procuratore;
- a coloro i quali, seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società. La previsione, di portata residuale, è finalizzata a conferire rilevanza al dato fattuale, in modo da ricomprendere, tra gli autori dei reati anche coloro che, compiendo determinate operazioni, agiscono concretamente sulla gestione della società;
- ai lavoratori subordinati della Società, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale, nonché ai dipendenti distaccati dalla o alla controllante;
- a chi, pur non appartenendo alla Società, opera su mandato o nell'interesse della medesima (consulenti, collaboratori, partner, fornitori, ecc.).

Il Modello costituisce un riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività, in qualità di fornitori di beni, servizi e lavori, consulenti, partners nelle associazioni temporanee o società con cui la Società opera.

1.7 Elementi fondamentali del Modello

Le regole comportamentali contenute all'interno del Codice Etico costituiscono parte integrante del presente Modello, e si integrano con quelle presenti nello stesso sebbene quest'ultime abbiano

una portata differente per la finalità che intendono perseguire in attuazione delle disposizioni del Decreto.

Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato allo scopo di esprimere dei principi di "deontologia aziendale" che la Società riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti e dei diversi portatori di interesse della Società (ad es. fornitori, partner, clienti, Pubblica Amministrazione, ecc.);
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi a vantaggio dell'azienda, possano comportare una responsabilità amministrativa della stessa in base alle disposizioni del Decreto medesimo).

1.8 Codice Etico e Modello 231

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico che ne costituisce parte integrate pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice stesso. Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale allo scopo di esprimere dei principi di "deontologia aziendale" che la Società riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti e dei diversi portatori di interesse della Società (ad es. fornitori, partner, clienti, Pubblica Amministrazione, ecc.);
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi a vantaggio dell'azienda, possano comportare una responsabilità amministrativa della stessa in base alle disposizioni del Decreto medesimo).

ORGANISMO DI VIGILANZA

L'art. 6, comma 1, del Decreto prevede che la funzione di vigilare e di curare l'aggiornamento del Modello sia affidata ad un Organismo di Vigilanza interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti a esso rimessi.

In nessun caso viene nominato componente dell'Organismo di Vigilanza, e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o dagli uffici direttivi delle persone giuridiche ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di patteggiamento, per aver commesso uno dei reati previsti dal Decreto.

Il componente dell'Organismo di Vigilanza è scelto tra soggetti che non abbiano rapporti di parentela con il Management della Società, che ne possano compromettere l'indipendenza di giudizio.

Laddove sia nominato un componente esterno, lo stesso non dovrà avere rapporti commerciali con la Società che possano configurare ipotesi di conflitto di interessi.

All'Organismo di Vigilanza sono attribuiti autonomi poteri di spesa che prevedono l'impiego di un budget annuo adeguato, approvato con provvedimento del Branch Manager.

In particolare, la composizione dell'Organismo di Vigilanza deve garantire i seguenti requisiti:

- *autonomia e indipendenza*: detto requisito è assicurato dall'assenza di un riporto gerarchico all'interno dell'organizzazione, dalla facoltà di reporting al Branch Manager), dalla composizione dell'Organismo di Vigilanza il cui componente non si trova in una posizione, neppure potenziale, di conflitto di interessi con la Società né è titolare all'interno della stessa di funzioni di tipo esecutivo;
- *onorabilità e professionalità*: requisito garantito dal bagaglio di conoscenze professionali, tecniche e pratiche, di cui dispone il componente dell'Organismo di Vigilanza.
- *continuità d'azione:* con riferimento a tale requisito, l'Organismo di Vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale della Società.

Al fine di garantire il rispetto di quest'ultimo requisito attraverso la "continuazione" dei meccanismi adottati in materia di D. Lgs. 231 prima della Fusione, la Società ha scelto di mantenere - fino alla scadenza dell'incarico - l'Organismo di Vigilanza precedentemente nominato, senza necessità di nuova validazione, in conformità di quanto previsto dalla normativa applicabile (cfr. in particolare gli artt. dal 2501 al 2505-quater e l'art. 2504 bis c.c. che non contiene più il riferimento all'effetto estintivo) e di quanto affermato dalla Suprema Corte di Cassazione in

materia, in caso di fusione la società incorporante subentra nella titolarità dei rapporti giuridici attivi e passivi, anche processuali, ed assume i diritti e gli obblighi delle società partecipanti alla fusione divenendo il nuovo centro di imputazione e di legittimazione dei rapporti giuridici già riguardanti i soggetti incorporati.

In particolare sul tema si richiamano le seguenti pronunce della Suprema Corte:

- Cass. 24 marzo 2006 n. 6686: il soggetto incorporato non si estingue, dato che i suoi interessi pregressi sono tutelati dal nuovo soggetto nato dalla fusione;
- Cass. 18 aprile 2012 n. 6058: la fusione tra società non determina, nella fattispecie per incorporazione, l'estinzione della società incorporata, né crea un nuovo soggetto di diritto nell'ipotesi di fusione paritaria, ma attua l'unificazione mediante l'integrazione reciproca delle società partecipanti alla fusione;
- Cass. n. 24026/2015; Cass. n. 10653/2010: il concetto di fusione: rappresenta l'operazione societaria che si deve qualificare come una "vicenda meramente evolutiva - modificativa dello stesso soggetto giuridico" che conserva la propria identità pur in un nuovo assetto organizzativo.

1. Identificazione dell'Organismo di Vigilanza e cause di ineleggibilità

Non possono essere nominati membri dell'Organismo e se nominati decadono dall'ufficio:

1. coloro che incorrono nelle cause di ineleggibilità e decadenza previste dall'articolo 2382c.c. (interdizione, inabilitazione, fallimento, interdizione - anche temporanea - dai pubblici uffici, incapacità a esercitare uffici direttivi);
2. il coniuge, i parenti e gli affini entro il quarto grado degli amministratori esecutivi della Società, gli amministratori esecutivi, il coniuge, i parenti e gli affini entro il quarto grado degli amministratori delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo;
3. coloro che sono stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria, salvi gli effetti della riabilitazione;
4. coloro che sono stati condannati con sentenza irrevocabile ovvero hanno concordato la pena ai sensi degli artt. 444 e ss. c.p.p. in relazione ad uno dei reati previsti dal D. Lgs. n. 231/2001 salvi gli effetti della riabilitazione.

I componenti dell'Organismo devono possedere le capacità, conoscenze e competenze professionali indispensabili allo svolgimento dei compiti ad essi attribuiti, nonché i requisiti di onorabilità, indipendenza e professionalità. L'Organismo può avvalersi, per l'espletamento dei suoi compiti di consulenti esterni, ferma restando la sua responsabilità in via esclusiva della vigilanza sul funzionamento e l'osservanza del Modello e della cura del suo aggiornamento.

All'Organismo di Vigilanza sono attribuiti autonomi poteri di spesa che prevedono l'impiego di un budget annuo adeguato, approvato dal Branch Manager.

2. Poteri e funzioni dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono affidati i seguenti compiti:

- vigilare sul funzionamento e osservanza del Modello;
- curarne l'aggiornamento.

Tali compiti sono svolti dall'Organismo attraverso le seguenti attività:

- vigilanza sulla diffusione nel contesto aziendale della conoscenza, della comprensione e dell'osservanza del Modello;
- vigilanza sull' effettività del Modello, con particolare riferimento ai comportamenti riscontrati nel contesto aziendale, verificandone la coerenza rispetto ai principi di comportamento e di controllo definiti nel presente Modello;
- disamina dell'adeguatezza del modello, ossia dell'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal Decreto;
- analisi circa il mantenimento nel tempo dei requisiti di solidità e funzionalità del modello
- formulazione di proposte di aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e/o adeguamenti dello stesso, in relazione alle mutate condizioni legislative e/o aziendali;
- segnalazione, anche documentale, al Branch Manager di eventuali violazioni accertate del modello organizzativo che possano comportare l'insorgere della responsabilità in capo alla Società.

Nello svolgimento di dette attività, l'Organismo provvederà ai seguenti adempimenti:

- collaborare con la direzione aziendale competente nella programmazione ed erogazione di un piano periodico di formazione volto a favorire la conoscenza delle prescrizioni del Modello;
- documentare lo svolgimento dei suoi compiti;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello.

Al fine di consentire all'Organismo la miglior conoscenza in ordine all'attuazione del Modello, alla sua efficacia e al suo effettivo funzionamento, nonché alle esigenze di aggiornamento dello stesso, è fondamentale che l'Organismo di Vigilanza operi in stretta collaborazione con le aree aziendali.

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo è dotato dei poteri di seguito indicati:

- accedere liberamente, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D. Lgs. 231/2001;
- disporre che i Destinatari forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare e approfondire aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- ricorrere a consulenti esterni nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello.

3. Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Decreto enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza. Detti flussi riguardano tutte le informazioni e i documenti che devono essere portati a conoscenza dell'Organismo di Vigilanza, secondo quanto previsto dai protocolli adottati e nelle singole Parti Speciali del Modello.

Per ciascuna area a rischio reato è identificato un responsabile interno che dovrà, tra l'altro, fornire all'OdV, almeno con cadenza semestrale, i flussi informativi così come definiti dall'Organismo stesso. Anche nel caso in cui, nel periodo selezionato, non vi siano state segnalazioni significative da comunicare all'OdV, allo stesso dovrà essere inviata una segnalazione negativa.

Sono stati inoltre istituiti precisi obblighi gravanti sugli organi sociali e sul personale, in particolare:

- i destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni o presunte violazioni delle prescrizioni del Modello o fattispecie di reato.
- gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello.

Oltre alle informazioni sopraindicate, devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

(i) i piani di comunicazione e formazione sui principi e i contenuti del Decreto e del Modello di organizzazione gestione e controllo;

(ii) i piani e i risultati delle attività di controllo e di audit, in relazione a processi e attività rilevanti ai sensi del presente Modello;

(iii) gli eventuali procedimenti disciplinari avviati per violazioni del Modello e i relativi provvedimenti sanzionatori o di archiviazione, con le relative motivazioni;

(iv) i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra Autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per ipotesi di reato di cui al d. lgs. 231/01, che riguardino direttamente o indirettamente la Società;

(v) le richieste di assistenza legale inoltrate dai componenti gli organi sociali, dai dirigenti e/o dagli altri dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto, che riguardino direttamente o indirettamente la Società;

(vi) eventuali ispezioni, accertamenti e visite promossi dalla Pubblica Amministrazione o da altri Enti competenti nei confronti della Società e i relativi contenziosi in essere;

(vii) modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;

(viii) segnalazione di infortuni gravi, rientrando in tale categoria quegli infortuni sul lavoro con prognosi superiore ai 40 giorni occorsi a dipendenti, appaltatori, subappaltatori e/o collaboratori presenti nei luoghi di lavoro della Società.

I destinatari del presente Modello possono, inoltre, trasmettere all'Organismo di Vigilanza indicazioni e suggerimenti relativi all'attuazione, all'adeguatezza e all'aggiornamento del Modello Organizzativo.

Al fine di agevolare il flusso informativo verso l'Organismo di Vigilanza è istituito un canale informativo dedicato al quale trasmettere i flussi informativi sopraindicati, costituito da un indirizzo di posta elettronica dedicato.

L'Organismo di Vigilanza raccoglierà e valuterà tutte le informazioni e le segnalazioni pervenutegli.

È rimesso alla discrezionalità dell'Organismo di Vigilanza valutare, sulla base delle segnalazioni ricevute, le iniziative da assumere. In particolare, potrà convocare, qualora lo ritenga opportuno, sia il segnalante per ottenere maggiori informazioni sia l'eventuale presunto autore della violazione, dando inoltre luogo a tutti gli accertamenti e le indagini che ritenga necessarie per appurare la fondatezza della segnalazione.

Le segnalazioni dovranno essere in forma scritta. Pertanto, è obbligo dell'Organismo di Vigilanza agire in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, fatti salvi gli obblighi di legge a tutela dei diritti della Società e dei terzi, assicurando l'anonimato del segnalante e la riservatezza dei fatti dal medesimo segnalati.

Tutte le informazioni, la documentazione e le segnalazioni raccolte nell'espletamento dei compiti istituzionali devono essere archiviate e custodite, per almeno cinque anni, dall'Organismo di Vigilanza, avendo cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

5. Flussi informativi dell'Organismo di Vigilanza

L'Organismo di Vigilanza riporta al Branch manager:

1) tempestivamente in caso di informazioni su violazioni del Modello o situazioni a rischio reato 231/01 pervenute dai Referenti interni o emerse all'esito delle attività di verifica;
2) tempestivamente per l'introduzione di nuovi reati presupposto nel catalogo dei reati 231 configurabili all'interno della Società o per modifiche della struttura societaria che richiedono un aggiornamento del Modello;
3) semestralmente sugli esiti delle attività svolte tramite una relazione scritta.

Il Branch manager ha l'obbligo di riportare al Consiglio di Amministrazione e/o al Management (in particolare al Chief Executive Officer/ Deputy Chief Executive Officer) della "Casa Madre" (Opel Bank SA):

1) tempestivamente le informazioni di cui al punto 1);
2) semestralmente sulle attività di cui al punto 2) e 3).

Nel caso in cui le informazioni relative a violazioni del Modello o a situazioni a rischio di reato dovessero coinvolgere il Branch Manager, l'OdV ha la facoltà di relazionare direttamente al Consiglio di Amministrazione e/o al Management (in particolare al Chief Executive Officer/ Deputy Chief Executive Officer) della Casa Madre.

GOVERNANCE ORGANIZZATIVA

1. Cenni su OPEL BANK S.A.

Opel Bank Italia è una succursale di Opel Bank Società anonima (société anonyme) di diritto francese il cui oggetto sociale consiste in:

- tutte le operazioni trattate e disciplinate dalle disposizioni del codice monetario e finanziario francese relative all'attività e al controllo delle istituzioni finanziarie, in particolare il finanziamento di operazioni di locazione, locazione-vendita e locazione-affitto di macchinari e attrezzi di qualsiasi genere ad uso industriale, commerciale, agricolo, professionale o domestico, così come tutte le operazioni di carattere non bancario dettagliate all'articolo 3.2.7 del regolamento n. 2000.03 del 6 settembre 2000, incluse le attività di intermediazione assicurativa;

- la partecipazione della società in qualsiasi operazione che possa riguardare una qualsiasi delle sopracitate attività, mediante la costituzione di nuove società, conferimenti da parte di soci a responsabilità limitata, sottoscrizione o acquisto di titoli o diritti societari, fusioni, associazioni, accordi di joint venture e, in generale, tutte le operazioni industriali, commerciali, immobiliari e finanziarie associate, direttamente o indirettamente, in tutto o in parte, a uno qualsiasi degli scopi sociali ovvero a qualsiasi altro fine similare o correlato.

Opel Bank S.A. è una società autorizzata come istituto di credito e soggetta all'attività di supervisione dell'Autorità di Controllo Prudenziale e di Risoluzione (Autorité de Contrôle Prudentiel et de Résolution – "ACPR") e della Banca Centrale Europea ("BCE").

2. Modello di Governance

La Società è dotata di un **Branch Manager (institore)** che svolge funzioni generali di gestione e amministrazione della Società, nell'ambito e nei limiti dei poteri e delle deleghe allo stesso attribuiti dalla Casa Madre.

Il Branch Manager ha a sua volta ha nominato dei (sub)procuratori, a cui sono delegati determinati poteri per specifiche aree o attività.

Inoltre, all'interno di Opel Bank Italia sono costituiti i seguenti dipartimenti / strutture interne:

Corporate Lending: è l'unità organizzativa preposta all'istruttoria delle proposte di affidamento (ed al loro successivo monitoraggio) alla Rete di Concessionari, alla gestione dei pagamenti dei concessionari, dei clienti rental e fleet, nonché alla gestione ordinaria dei rapporti di affidamento nell'ottica di prevenzione e contenimento dei rischi creditizi. Il responsabile dell'area gestisce le sofferenze Corporate Lending.

Retail Acquisitions: è l'unità organizzativa preposta all'analisi del merito creditizio dei richiedenti appartenenti al segmento retail (istruttoria finanziamenti), ed all'acquisto dei contratti che ne derivano.

Collections: è l'unità organizzativa preposta al sollecito telefonico e al monitoraggio andamentale delle posizioni retail e delle performance delle agenzie di recupero esterne, oltre ad intervenire direttamente per i contratti in contenzioso che presentano particolari difficoltà di recupero, nonché alla gestione delle sofferenze retail affidate ad avvocati esterni.

Admin & Customer Service: è l'unità organizzativa preposta all'imputazione dei pagamenti rateali e al supporto della clientela. L'attività di Customer Service si struttura su due livelli operativi:

1) **primo livello**: che gestisce tutto il volume delle telefonate in entrata della clientela, per la risoluzione di problematiche di carattere generale. Tale attività operativa è esternalizzata ad una società che provvede a dirottare ai reparti di competenza tutte le questioni o necessità di carattere non generale.

2) **secondo Livello**: si occupa, invece, della risoluzione delle problematiche telefoniche e di clienti non in contenzioso, che vengono seguite da personale specializzato.

Finance: assicura le attività amministrativo-contabili, l'approvvigionamento dei fondi necessari per lo svolgimento dell'attività societaria e la gestione del sistema contabile interno, la predisposizione del Bilancio d'esercizio e delle situazioni infrannuali sia a fini civilistici e fiscali che infragruppo. E' responsabile, inoltre, della predisposizione delle segnalazioni periodiche di Vigilanza, della redazione del Business Plan e dell'analisi degli scostamenti rispetto al business plan.

Marketing: è l'unità organizzativa preposta all'attività di marketing e sviluppo di nuovi prodotti sia rateali che assicurativi, in collaborazione con l'unità Insurance, secondo quanto previsto dalla normativa IVASS. Garantisce il monitoraggio delle performance commerciali retail fornendo analisi e report commerciali alla direzione e al sales team. Gestisce la relazione con il costruttore sviluppando iniziative commerciali congiunte. Inoltre, questa l'unità sviluppa nuovi prodotti assicurativi, secondo quanto previsto dalla normativa IVASS. Gestisce la relazione con le Compagnie Assicurative partner garantendo altresì ilmonitoraggio delle performance commerciali.

Sales: è l'unità organizzativa preposta a supportare le concessionarie nel perseguimento degli obiettivi di volume della Società, in termini di contratti rateali e assicurativi. Le funzioni di Staff sono le funzioni di controllo, che riportano direttamente all'Organo con Funzioni di Gestione (funzioni di controllo di secondo livello) ed all'Organo con Funzioni di Supervisione Strategica (funzione Audit).

Compliance e Anti-money Laundering Officer: ha il compito di prevenire e gestire il rischio di non conformità alla normativa, eseguendo i relativi controlli di secondo livello. Il responsabile della funzione ricopre anche il ruolo di Responsabile antiriciclaggio e segnalazione delle operazioni sospette;

Risk Management: collabora alla definizione del sistema di gestione del rischio della Società e ne verifica il corretto funzionamento;

Audit (in outsourcing): assicura i controlli di terzo livello (controlli di revisione interna) garantendo la coerenza dei processi operativi in conformità alla missione aziendale, ai regolamenti interni, locali e dell Capogruppo, e alle disposizioni normative e di vigilanza;

Human Resources: svolge un ruolo di direzione strategica nello sviluppo e implementazione di iniziative e processi che riguardano tutti i dipendenti, in stretto allineamento con gli obiettivi operativi dell'organizzazione;

Information Technology: assicura che la società sia dotata delle funzionalità IT necessarie per supportare l'operatività e il raggiungimento degli obiettivi aziendali. Lavora a stretto contatto con la leadership aziendale per sviluppare una comprensione della strategia aziendale e delle priorità. Assicura che le esigenze locali IT siano garantite interfacciandosi con la direzione centrale IT.

La governance organizzativa di Opel Bank Italia si svolge nell'ambito di:

- Comunicazioni operative emanate dai responsabili delle Aree operative
- Mansionario
- Procedure

che costituiscono parte integrante del presente Modello.

***

Nell'analisi organizzativa preliminare all'aggiornamento del Modello 231/01 si è avuto cura di verificare che:

1) tutti i processi omogenei aventi rilevanza in termini gestionali sono ricondotti a un unico responsabile di riferimento collocato formalmente in organigramma con esplicite missioni e responsabilità;
2) l'organizzazione è tale da garantire chiarezza delle gerarchie, coordinamento, monitoraggio e rendicontazione periodica delle attività svolte;
3) a ciascun responsabile di funzione competono, oltre al coordinamento delle attività relative alla missione assegnata, la valutazione e gestione dei rischi inerenti, la misurazione delle performance, il reporting per linea gerarchica, la supervisione del personale assegnato.

3. Quadro regolatorio di riferimento

Opel Bank Italia svolge la propria attività all'interno di un quadro regolatorio di riferimento ampio e cogente.

In particolare, per quel che concerne l'attività finanziaria, è soggetta a titolo esemplificativo e non esaustivo alle seguenti disposizioni normative:

1) Circolare di Banca d'Italia n. 285 del 17 dicembre 2013 recante "Disposizioni di vigilanza per le banche" sezione VIII.
2) Circolare di Banca d'Italia n. 272 del 30 luglio 2008 recante "Vigilanza Bancaria e finanziaria "
3) Circolare di Banca d'Italia n. 154 del 22 novembre 1991 recante "Segnalazioni di vigilanza delle istituzioni creditizie e finanziarie".
4) Banca d'Italia - Comunicazione del 7 giugno 2011 recante la disciplina relativa "Nuova segnalazione sugli organi sociali (Or.So.). Istruzioni per gli intermediari"
5) D. Lgs. n. 209/05 - Codice delle Assicurazioni, come modificato dal decreto legislativo 21 maggio 2018, n. 68
6) Regolamento IVASS n. 40/2018 - Distribuzione assicurativa e riassicurativa.
7) Circolare Banca D'Italia del 28 Settembre 2009 sulla "Trasparenza delle operazioni e dei servizi bancari e finanziari; correttezza delle relazioni tra intermediari e clienti"
8) Disposizioni di Banca d'Italia del 18.06.2009 sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari.
9) Direttiva UE n. 849 del 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggi oo finaniamento del terrorismo
10) D.lgs 231/2007 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione"
11) Decreto Legislativo 22 giugno 2007, n. 109 "Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attivita' dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE"

Tali disposizioni legislative identificano gli obblighi e gli adempimenti di cui la Società è destinataria, i doveri di comunicazione nei confronti dei Regulator, le modalità di svolgimento e rendicontazione delle attività nonché i doveri di segnalazione di eventuali irregolarità.

Tali regole configurano di fatto un *sistema di prevenzione ex ante dei reati 231* in quanto limitano di fatto l'agire dei responsabili in relazione anche al sistema di controlli esterni che prevedono.

In quanto tali esse costituiscono parte integrante dei presidi indicati nel presente Modello.

4. Procedure operative interne

La Società ha adottato procedure operative che disciplinano lo svolgimento delle attività, tra cui a titolo esemplificativo:

- Procedura Business Plan
- Procedura nuovi prodotti
- Report Direzionali
- Local Organisation Note - Hub Italy
- Corporate Lending
- Elenco dei Sistemi informativi
- Procedura Bilancio
- Procedure per la produzione delle segnalazioni di vigilanza e dell'ICAAP
- Processo ICAAP
- Regolamento della Funzione Compliance
- Regolamento della Funzione Antiriciclaggio
- Regolamento Risk Management
- Regolamento Comitato Rischi
- Deleghe in materia di concessione del credito
- Procedura Antiriciclaggio e Antiterrorismo
- Italy Consumer Credit Procedures e Italy SME underwriting criteria
- Policy in materia di esternalizzazioni.

che estendono la loro valenza anche alla prevenzione dei reati 231/01.

5. Whistleblowing per le segnalazioni di illeciti e irregolarità

La legge del 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*" (c.d. Whistleblowing) ha modificato l'art. 6 del d. lgs. n.231/2001 introducendo l'obbligo di prevedere all'interno del Modello canali (anche informatici e comunque tali da garantire la riservatezza del segnalante) che consentano ai soggetti di cui all'art. 5 d. lgs. n. 231/2001 (ovvero ai soggetti apicali o subordinati) di effettuare segnalazioni riguardanti condotte illecite rilevanti ai fini del d. lgs. n. 231/2001.

In conformità a tale previsione Opel Bank Italia ha adottato la procedura *Whistleblowing*, che costituisce parte integrante del presente Modello.

In sintesi la procedura:

1) qualifica le segnalazioni da effettuare, quali quelle:
    a. penalmente rilevanti

   b. poste in essere in violazione dei Codici di comportamento (ad es. Codice etico, modello 231/01) o di altre disposizioni o regolamenti aziendali sanzionabili
   c. suscettibili di arrecare un pregiudizio patrimoniale o reputazionale a Opel Bank Italia o ai dipendenti o ad altri soggetti che svolgono la loro attività presso l'azienda
2) identifica i contenuti della segnalazione
3) indica le modalità e i destinatari della segnalazione. In particolare la segnalazione può essere indirizzata all'OdV

mediante:

   a. a mezzo del servizio postale o tramite posta interna in una busta chiusa che rechi all'esterno la dicitura "riservata/personale"
   b. verbalmente, mediante dichiarazione rilasciata e riportata a verbale da uno dei soggetti legittimati alla loro ricezione
4) illustra le attività di verifica sulla fondatezza della segnalazione
5) le modalità ddi archiviazione della documentazione
6) gli obblighi di riservatezza nei confronti di chi ha effettuato la segnalazione e i divieti di discriminazione nei confronti di questi.

SEZIONE A – REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE

La presente sezione è suddivisa come segue:

1. ***Reati e modalità di commissione***: richiama i reati nei confronti della P.A.[1] con un commento sulle modalità di commissione
2. ***Ruoli e responsabilità interne***; individua i ruoli e le responsabilità organizzative interne a presidio dei rischi
3. ***Processi sensibili e protocolli***; definisce le aree sensibili ai rischi reato, i protocolli di prevenzione adottati e gli obblighi informativi nei confronti dell'Organismo di Vigilanza
4. ***Protocolli per la gestione delle attività potenzialmente strumentali ai reati di corruzione o concussione***; definisce le regole di comportamento da adottarsi durante le attività potenzialmente strumentali alla commissione dei reati quali la gestione del personale, gli affidamenti di incarichi di consulenza, la gestione degli adempimenti societari e la gestione degli acquisti.

1. Reati e modalità di commissione

Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, il soggetto dopo aver ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta). Di conseguenza, poiché il reato si perfeziona nel momento in cui le somme, erogate dallo Stato o da altro ente pubblico, vengono spese per uno scopo diverso da quello inizialmente previsto, la condotta illecita può essere contestata anche a notevole distanza di tempo rispetto all'incasso del finanziamento.

[1] Per una migliore lettura della presente sezione si premettono di seguito le nozioni di Pubblica Amministrazione (d'ora innanzi PA), Pubblico Ufficiale (PU) e Incaricato di Pubblico Servizio (IPS). Per PA si intende, in estrema sintesi, l'insieme di enti e soggetti pubblici (Stato, Ministeri, Regioni, Province, Comuni ecc.) e talora privati (ad es. concessionari, amministrazioni aggiudicatrici, S.p.A. miste ecc.) e tutte le altre figure che svolgono in qualche modo attività pubblica, nell'interesse della collettività e quindi nell'interesse pubblico. Oggetto della tutela di legge è il regolare funzionamento della Pubblica Amministrazione di cui all'art. 97 della Costituzione nonché il prestigio degli Enti Pubblici, ovvero, nei casi di truffa, il patrimonio pubblico. La nozione di PU è fornita direttamente dal legislatore, all'art. 357 c.p., il quale identifica il "pubblico ufficiale" in "chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa", specificando che "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della Pubblica Amministrazione e dal suo svolgersi per mezzo dei poteri autoritativi e certificativi". I pubblici poteri qui in rilievo sono: il potere legislativo, quello giudiziario e, da ultimo, quelli riconducibili alla pubblica funzione amministrativa. Diversamente, l'art. 358 c.p. riconosce la qualifica di "incaricato di pubblico servizio" a tutti "coloro i quali, a qualunque titolo, prestano un pubblico servizio", intendendosi per tale "un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale". E' pertanto un IPS chi svolge una "pubblica attività", non riconducibile ad alcuno dei poteri sopra rammentati e non concernente semplici mansioni d'ordine e/o prestazioni d'opera meramente materiali ed, in quanto tali, prive di alcun apporto intellettuale e discrezionale. Esempio di IPS sono i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati. L'effettiva ricorrenza dei requisiti indicati deve essere verificata, caso per caso, in ragione della concreta ed effettiva possibilità di ricondurre l'attività di interesse alle richiamate definizioni, essendo certamente ipotizzabile anche che, soggetti appartenenti alla medesima categoria, ma addetti ad espletare differenti funzioni o servizi, possono essere diversamente qualificati proprio in ragione della non coincidenza dell'attività da loro in concreto svolta.

Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.)

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi, ovvero mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea. In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Tale ipotesi di reato si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n. 1, c.p.)

La fattispecie di reato punisce coloro i quali, al fine di trarre un ingiusto profitto, mediante artifizi o raggiri o inducendo taluno in errore, ottengono vantaggi patrimoniali ai danni dello stato o di altro ente pubblico.

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche. Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici. Il reato in questione può facilmente concorrere con quello di cui all'art. 316-bis, in quanto può concretizzare condotte prodromiche all'erogazione del contributo distratto dalla destinazione prevista.

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ipotesi in cui un dipendente concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che da tale comportamento derivi in qualche modo un vantaggio per la società).

Corruzione per l'esercizio della funzione e corruzione per un atto contrario ai doveri d'ufficio (artt. 318-319 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un

vantaggio in favore dell'offerente). L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara). Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

Circostanze aggravanti (art. 319-bis)

La pena è aumentata se il fatto di cui all'articolo 319 ha per oggetto il conferimento di pubblici 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.

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

Tale ipotesi di reato si configura nel caso in cui i fatti indicati negli artt. 318 e 319 c.p. siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. Il reato di corruzione in atti giudiziari può essere commesso nei confronti di giudici o membri del Collegio Arbitrale competenti a giudicare sul contenzioso/arbitrato nell'interesse dell'Ente (compresi gli ausiliari e i periti d'ufficio), e/o di rappresentanti della Pubblica Amministrazione, quando questa sia una parte nel contenzioso, al fine di ottenere illecitamente decisioni giudiziali e/o stragiudiziali favorevoli.

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

Tale ipotesi di reato punisce la condotta dei soggetti apicali o dei soggetti subordinati che siano indotti a versare o promettere denaro o altra utilità, in ragione dell'abuso di potere del pubblico ufficiale o l'incaricato di pubblico servizio.

Pene per il corruttore (art. 321 c.p.)

Le pene stabilite nel primo comma dell'articolo 318, nell'art. 319, nell'art. 319-bis, nell'articolo 319-ter e nell'art. 320 c.p. in relazione alle suddette ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.

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

Tale ipotesi di reato si configura nei confronti di chiunque offra o prometta denaro o altra utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio che rivesta la qualità di pubblico impiegato per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri e tale offerta o promessa non sia accettata.

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.)

Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a 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.

Le disposizioni degli articoli 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

1) alle persone indicate nel primo comma del presente articolo;

2) 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, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

Traffico di influenze illecite

Tale reato punisce la condotta di chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, 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 un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

Si tratta di un reato introdotto dalla legge 190/2012 e modificato dalla L. 3 del 2019che punisce i soggetti terzi che intermediano nell'opera di corruzione tra il corrotto ed il corruttore.

Il comportamento antigiuridico sanzionato, dunque, si verifica nel momento in cui viene pattuita la dazione di un bene o altra utilità in cambio dell'esercizio di un'influenza sul pubblico ufficiale deputato alle decisioni amministrative favorevoli al soggetto che promette o dà.

Le condotte che rientrano nell'alveo del reato possono essere di due tipologie differenti: il traffico di influenze gratuito, nel quale il committente dà o promette denaro destinato alla corruzione del P.U. (il denaro o il vantaggio patrimoniale dato o promesso dal committente al mediatore è utilizzato per remunerare il pubblico agente per il compimento di un atto contrario ai doveri di ufficio o per l'omissione o il ritardo di un atto del suo ufficio), realizzando così il delitto di corruzione propria o di corruzione in atti giudiziari; traffico di influenze oneroso, laddove il committente remunera il mediatore affinché quest'ultimo realizzi una illecita influenza sul pubblico agente.

***

Onde limitare le situazioni a rischio di *corruzione* che potrebbero insorgere già dall'istaurarsi di un rapporto a carattere interlocutorio o informativo, la Società osserva le seguenti regole:

- a chiunque (consiglieri, direttori, dipendenti, consulenti e terzi) intrattenga rapporti con la P.A. in rappresentanza della Società deve essere formalmente conferito potere in tal senso ;
- i contratti con consulenti delegati a intrattenere rapporti per conto della società con la Pubblica Amministrazione devono essere definiti per iscritto e i compensi in loro favore devono trovare adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
- di tutte le richieste informative e di tutti i rapporti rilevanti intrattenuti per iscritto con le Pubbliche Amministrazioni in rappresentanza della Società si dovrà conservare adeguato supporto documentale a disposizione dell'Organismo di Vigilanza;
- in tutti i rapporti anche episodici, tutti i dipendenti sono tenuti ad attenersi alle regole indicate nel Modello e nel Codice Etico
- qualunque criticità, conflitto o contestazione dovessero sorgere nell'ambito dei rapporti con la P.A. deve essere comunicata ai Referenti interni i quali, se del caso, provvederanno a darne comunicazione all'Organismo di Vigilanza.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)

La fattispecie in esame è diretta a reprimere le ipotesi di illecito arricchimento conseguito alterando, in qualunque modo, il funzionamento di un sistema informatico o telematico, condotta integrata quando si attui una interferenza con il regolare svolgimento di un processo di elaborazione dati al fine di ottenere uno spostamento patrimoniale ingiustificato. Altra modalità

di realizzazione del reato consiste nell'intervento abusivo su dati, programmi o informazioni contenuti in un sistema informatico o telematico, intervento attraverso il quale l'agente procura a sé o ad altri un ingiusto profitto con danno altrui. Da notare che la fattispecie in esame viene presa in considerazione dal Decreto soltanto nell'ipotesi in cui il fatto sia commesso in danno dello Stato o di altro Ente Pubblico.

In merito alla possibilità di commissione del reato di frode informatica si può ipotizzare l'alterazione di registri informatici tenuti da Pubbliche Amministrazioni per far risultare esistenti condizioni essenziali per ottenere contributi pubblici; ovvero per modificare dati fiscali o previdenziali di interesse dell'azienda, già trasmessi alla Pubblica Amministrazione competente. Un'ulteriore ipotesi potrebbe essere quella di violazione di un sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

2. Ruoli e responsabilità interne

I ruoli che concorrono a realizzare condizioni di prevenzione e identificazione delle situazioni a rischio di reato, oltre a quello dell'Organismo di Vigilanza, sono i seguenti:

- Branch Manager
- Director Finance
- Director Sales & Marketing
- Director Operations
- Accounting Manager
- Sales Manager
- Marketing Manager
- Insurance Manager
- Operations Manager
- Legal
- HR
- Compliance & AML Manager
- Risk Manager
- Corporate Secretary
- i Referenti interni dell'OdV
- tutte le funzioni che per ragioni di servizio intrattengono rapporti con la P.A.

Sono comunque tenuti a informare tempestivamente i diretti superiori ovvero gli organi deputati istituzionalmente al controllo tutti coloro che sono in possesso di informazioni relative al rischio di commissione di reato o alla sua avvenuta consumazione.

Prima di entrare nel merito dei processi sensibili e dei presidi in atto, onde limitare le situazioni a rischio di reato nei confronti della PA che potrebbero insorgere già dall'instaurarsi di un rapporto

a carattere interlocutorio o informativo, si riporto uno *standard cautelativo generale*, al cui rispetto sono tenuti tutti i destinatari del Modello.
Nei confronti con la P.A. è espressamente fatto divieto di:

1) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate;
2) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle;
3) porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato;
4) effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia a pubblici funzionari;
5) distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice etico, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico, o la brand image della Società. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;
6) accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto;
7) effettuare prestazioni in favore dei consulenti, dei Partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;
8) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
9) alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;
10) elargire, promettere o dare denaro o altra utilità a giudici, arbitri, funzionari di cancelleria, periti, testimoni, ecc., ovvero a persone comunque indicate da codesti soggetti, nonché adottare comportamenti – anche a mezzo di soggetti Terzi (es. professionisti esterni) - contrari alla legge e ai presidi aziendali, per influenzare indebitamente le decisioni dell'organo giudicante ovvero le posizioni della Pubblica Amministrazione, quando questa sia una parte nel contenzioso;

11) favorire indebitamente gli interessi della Società inducendo con violenza o minaccia, o, alternativamente, con offerta di danaro o altra utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale.

3. Processi sensibili

All'esito dell'attività di valutazione dei rischi svolta ai sensi del Decreto sono emerse come principali attività sensibili:

1. la gestione dei rapporti con le Autorità di Vigilanza in quanto succursale italiana di banca estera;
2. la gestione del precontenzioso, contenzioso e delle visite ispettive da parte dei Pubblici Ufficiali.

3.1 Gestione dei rapporti con le Autorità di Vigilanza in quanto succursale di Banca Estera

La società, in qualità di succursale di Banca estera, è soggetta solo ed esclusivamente ad alcuni obblighi di segnalazione e comunicazione previsti dalle Autorità di Vigilanza preposte (Banca d'Italia, IVASS, UIF, ecc.).

Si premette che:

- per "segnalazioni" si intendono le informazioni di natura periodica che la Società è tenuta a fornire alle Autorità di vigilanza secondo quanto previsto dalle Circolari e Regolamenti, quali quelle relative all'esercizio delle funzioni di vigilanza (a titolo esemplificativo non esaustivo le segnalazioni di operazioni sospette, o le segnalazioni alla Centrale dei Rischi)
- per "comunicazioni" le informazioni inviate in seguito a richiesta da parte delle Autorità che possono riguardare, a titolo esemplificativo, ulteriori chiarimenti a seguito delle segnalazioni.

Nell'ambito della gestione di tali segnalazioni o comunicazioni, la Società potrebbe teoricamente incorrere nei reati di truffa, corruzione, istigazione alla corruzione, traffico di influenze illecite, al fine di ottenere un illecito vantaggio, quale ad esempio la mancata comminazione di sanzioni per irregolarità riscontrate.

A presidio, oltre allo standard cautelativo generale contenuto nel par. 2:

1) è stato nominato il Comitato Rischi, composto da Risk Manager, Finance Director, Director Operations, Sales Director, che ha il compito di:

- monitorare l'andamento dei rischi complessivi cui è esposta la Società e informare costantemente il Branch Manager che valuterà in base ai limiti della delega a lui conferita, se darne comunicazione anche al Consiglio di Amministrazione e/o al Management della Casa Madre;
- valutare l'adeguatezza dei presidi organizzativi a fronte dei rischi;

- proporre al Branch Manager le soluzioni per l'adeguamento del sistema di gestione e controllo dei rischi.

2) sono state adottate le procedure "Procedura per la produzione delle segnalazioni di vigilanza e dell'ICAAP" e "Procedura di gestione delle segnalazioni di Operazioni sospette" che richiamano ruoli e responsabilità interne, nonché le modalità di svolgimento dei processi di segnalazione.

Per quanto concerne tutti gli altri obblighi riguardanti le segnalazioni alle Autorità di Vigilanza, gli stessi vengono eseguiti, previa verifica e validazione della funzione Compliance, dalla Funzione Corporate Secretary.

Su base semestrale a cura della medesima funzione, viene redatto un report di tutte le segnalazioni effettuate per portarne a conoscenza l'OdV.

In caso di richiesta di ulteriori informazioni da parte dei destinatari della comunicazione viene avvisato il Branch Manager che, in base al tipo di informazione richiesta, valuta se informare il Consiglio di Amministrazione e/o il Management della Casa Madre.

Quanto alle segnalazioni di operazioni sospette, laddove i responsabili delle Aree che gestiscono l'erogazione e le operazioni sul consumo riscontrino un'anomalia, trasmettono tempestivamente la documentazione al responsabile Compliance & AML il quale, effettua la verifica rafforzata e ne comunica gli esiti all'Autorità di Vigilanza.

3.3 Gestione del precontenzioso e del contenzioso con la Pubblica Amministrazione

Si precisa che per *precontenzioso* si intende la constatazione da parte di un Responsabile Interno, sulla base di circostanze oggettive (natura delle informazioni assunte, ispezioni, verbali di accertamento, notifiche, diffide ed ogni altro atto preliminare di indagine da parte di Pubblico Ufficiale o Pubblica Amministrazione in generale), del potenziale rischio che la società possa essere coinvolta in un contenzioso avverso la P.A.

Pertanto si collocano in questo ambito:

a) eventuali inadempimenti sanzionabili dall'Autorità competente che pertanto, possono generare un potenziale rischio di corruzione di Pu al fine di evitare o attenuare il rischio di irrogazione di provvedimenti da parte della medesima autorità tutte le attività svolte in ottemperanza a norme generali, tra le quali sono considerate sensibili quelle che, suscettibili di inadempimenti,possono per ciò stesso generare un precontenzioso, il quale a sua volta comporta un potenziale rischio di corruzione di pubblici ufficiali in fase di verifica al fine di evitare o attenuare l'irrogazione dei provvedimenti e delle sanzioni previste dalla disciplina in materia in caso di rilievi di non conformità;
b) i rapporti con le Autorità pubbliche di Vigilanza in sede di ispezione, contestazione e accertamenti per gli aspetti che riguardano la conformità a norme e regolamenti;

c) la gestione della corrispondenza sensibile[2], in relazione alla quale la Società adotta i seguenti presidi:
   1. tutta la posta sensibile in entrata e in uscita è protocollata in giornata con l'apposizione di data e numero progressivo da parte dell'addetto amministrativo
   2. le lettere in partenza sono compilate su carta intestata della Società con l'indicazione della Funzione emittente, la qualifica e il nome per esteso del firmatario
   3. la posta sensibile viene sempre firmata secondo i poteri e le competenze definite dalla Società
   4. è competenza dell'Organismo di vigilanza verificare periodicamente il registro del protocollo utilizzato per l'archiviazione della posta sensibile in entrata ed in uscita e ove necessario ottenerne copia e ogni necessaria informazione
   5. tutta la corrispondenza gestita per e-mail che impegna la Società verso i pubblici uè sempre seguita da una conferma scritta.

Al fine di assicurare la necessaria trasparenza si dispone che per ogni visita effettuata da PU in qualunque sede di pertinenza di Opel Bank Italia deve essere data tempestiva comunicazione al superiore gerarchico.

Sulla base di circostanze oggettive, valutando la ragionevole certezza che ci siano i presupposti, il Responsabile della funzione operativa o il Referente interno sono tenuti a constatare lo stato di precontenzioso e a darne tempestiva comunicazione al superiore gerarchico, predisponendo una relazione scritta relativamente a tutti i potenziali elementi rilevanti che hanno influenzato tale decisione e istruendo un apposito fascicolo contenente la documentazione relativa alla gestione del precontenzioso e i rapporti intrattenuti in merito con la Pubblica Amministrazione competente in materia.

Nel caso in cui la vertenza non venga definita, si procede ad attivare l'iter per il contenzioso in giudizio.

Nella gestione di qualunque contenzioso, al fine di scongiurare il rischio di corruzione in atti giudiziari, Opel Bank Italia adotta i seguenti comportamenti:

a) i dipendenti e i collaboratori si astengono da:

- dare o promettere denaro o altre utilità a pubblici funzionari o a incaricati di un pubblico servizio o a persone dagli stessi indicati in modo da influenzare l'imparzialità del loro giudizio;

[2] Qualunque comunicazione in arrivo dalla Pubblica Amministrazione che implichi un comportamento attivo da parte della Società in termini informativi, operativi, oblativi, attestativi che, ove non messo in atto, può innescare l'insorgere di provvedimenti, diffide ad adempiere o precontenziosi. Qualunque comunicazione in uscita che impegna la Società in quanto controparte inadempiente (o presunta tale) a norme istituzionali (Inps, Inpdai, Ministero delle Finanze, ecc) e/o a adempimenti commerciali con controparti pubbliche e in ogni caso qualunque risposta alla posta sensibile ricevuta.

- inviare documenti falsi, attestare requisiti inesistenti o fornire garanzie non rispondenti al vero;
- porre in essere qualsiasi tipo di condotta illecita idonea a favorire o danneggiare una parte nel processo;
- promuovere, assecondare o tacere l'esistenza di un accordo illecito o di una qualsiasi irregolarità o distorsione nelle fasi processuali.

b) è compito del Responsabile dell'Area Legale:

- curare l'istruttoria generale del contenzioso e mantenere i rapporti con i legali esterni che assistono la Società nel contenzioso stesso, secondo le procedure interne previste a tal riguardo di volta in volta vigenti;
- conservare tutta la documentazione a disposizione dell'OdV;
- aggiornare periodicamente l'OdV e il Branch Manager (o per il tramite del Branch Manager, il Consiglio di Amministrazione della Casa Madre) sullo status dei contenziosi e fornire assistenza nel valutare le azioni appropriate.

4. Protocolli per la gestione delle attività potenzialmente strumentali alla commissione del reato di corruzione o concussione

Sono considerate sensibili, in quanto strumentali alla commissione dei reati di corruzione, le attività inerenti a:

1. Gestione attività di selezione ed assunzione del personale, dei compensi o di eventuali sistemi premianti.
2. Gestione delle risorse finanziarie
3. Gestione degli acquisti

La gestione delle attività strumentali elencate dovrà essere improntata ai seguenti principi di comportamento.

4.1 Gestione attività\ di selezione ed assunzione del personale, dei compensi o di eventuali sistemi premianti.

Nella Gestione del processo di selezione ed assunzione del personale Opel Bank Italia potrebbe ipoteticamente incorrere nel reato di corruzione mediante l'assiunzione di un soggetto collegato a Pubblico Ufficiale al fine di ottenere un illecito vantaggio.
A presidio di tale rischio la Società ha adottato la procedura di gruppo la quale prevede che:

- il responsabile dell'area che necessita dell'introduzione di una nuova risorsa, chiede l'autorizzazione al Team HR in base alle deleghe autorizzative previste dalla Casa Madre che comprendono sempre il Branch Manager e il responsabile risorse umane;

- dopo aver ottenuto l'autorizzazione del Team, il responsabile dell'area predispone la job description e viene contattato il responsabile della selezione che , in caso di profili con particolari caratteristiche, incarica una società di recruiting;
- le candidature vengono visualizzate su un portale informatico appositamente creato, che permette di gestire tutte le fasi di selezione;
- in sede di partecipazione alla selezione, al candidato vengono richieste informazioni su eventuali incompatibilità o conflitti di interessi che potrebbero pregiudicare l'eventuale assunzione;
- il responsabile interessato sulla base delle candidature ricevute seleziona i soggetti da intervistare;
- successivamente il candidato viene contattato e intervistato secondo i criteri stabiliti dalla procedura di gruppo.
- il candidato selezionato, prima di procedere con l'assunzione, dovrà produrre la documentazione attestante quanto dichiarato in sede di adesione all'offerta.
- il contratto viene predisposto dal responsabile risorse umane, sottoposto al vaglio del consulente del lavoro ove opportuno e, solo dopo tale verifica viene approvato dal Branch Manager.

4.2 Gestione delle risorse finanziarie

Nella gestione delle risorse finanziarie Opel Bank Italia osserva i seguenti principi:

Per i pagamenti:

- la separazione di responsabilità tra chi ordina un bene o un servizio e chi autorizza il pagamento,
- il divieto di autorizzare un pagamento non supportato da adeguata documentazione, il divieto di effettuare pagamenti per cassa al di sopra dei limiti di legge,
- obbligo di indicare sugli assegni il destinatario e di apporre la clausola non trasferibile o la barratura;
- la centralizzazione di tutti i pagamenti;
- la tracciabilità degli atti e delle singole fasi del processo con specifico riferimento all'annullamento dei documenti che hanno già originato un pagamento;
- il divieto di effettuare cambi di assegni o altri titoli di credito.

Per gli incassi:

- l'incasso accentrato principalmente a mezzo banca; riscontri periodici tra i dati contabili e le risultanze dei terzi.

Per la gestione dei conti bancari:

- ❖ l'autorizzazione per l'apertura e chiusura dei conti bancari al Branch Manager o altro soggetto delegato; riconciliazione degli estratti conto con le risultanze contabili e accertamenti della rapida sistemazione delle poste in riconciliazione da parte di responsabili che non possono operare con le banche;
- ❖ gestione tecnica delle condizioni bancarie da parte di soggetti professionali aziendali diversi da coloro che hanno il potere di operare con le banche;
- ❖ divieto di tenere risorse finanziarie non depositate sui conti correnti bancari della Società a eccezione delle piccole casse.

4.3 Gestione degli acquisti

Nei rapporti con i fornitori è fatto obbligo di:

- rispettare valori e parametri di obiettività imparzialità e correttezza
- valutare accuratamente le offerte ricevute con criteri oggettivi
- non discriminare o estromettere i fornitori di livello primario
- prevedere la verifica della sede residenza o domicilio in paesi black list
- garantire la congruità del prezzo con il valore del servizio
- osservare le procedure operative interne per la selezione del fornitore
- rispettare i principi di documentabilità, tracciabilità e verificabilità per i quali il Responsabile procurement si accerta sulla corrispondenza tra la richiesta d'acquisto ed il budget disponibile, motivando validamente tutti i provvedimenti di affidamento diretto.

Ad ulteriore Presidio la Società ha adottato la procedura operativa di gruppo denominata "Vendor Due Diligence" la quale prevede che:

1) i responsabili delle aree operative esprimono le necessità di acquisto di un servizio o di un prodotto, con richiesta scritta al Local Procurement;
2) Il Local Procurement compila un apposito modulo che condivide con il responsabile Compliance;
3) All'esito della verifica, la richiesta di acquisto dev'essere autorizzata Manager Direcor, (in alternativa se di importo inferiore a €10.000 da un soggetto a cui è stata attribuita la delega) e ritrasmessa al Responsabile richiedente;
4) Il Responsabile interessato, sulla base di una ricerca di mercato, chiede le offerte di almeno 2 fornitori.
5) Ottenute le offerte, il Local Procurement svolge un controllo sull'affidabilità (tramite richiesta delle visure camerali aggiornate, certificazioni di regolarita contributiva) e, per i beni/servizi con valore superiore a € 10.000 effettua anche un risk assesment con la valutazione di tutti i rischi legati alla prestazione
6) Una volta selezionato il fornitore con l'offerta più vantaggiosa per l'azienda,l'Area legale provvede a redigere il contratto che verrà sottoscritto dal Fornitore e dal Manager Director.

7) gli acquisti di importo inferiore a €10.000 possono essere autorizzati dai consiglieri di amministrazione dotati di apposita procura,

In caso di servizi di gestione di attività la cui esecuzione possa compromenttere gravemente:

i) i risultati finanziari, la solidità o la continuità della attività dell'intermediario finanziario o la capacità dell'intermediario di conformarsi alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;

Ovvero,

- riguarda attività sottoposte a riserva di legge;

- riguarda processi operativi delle funzioni aziendali di controllo;

- ha un impatto significativo sulla gestione dei rischi aziendali.

La necessità di acquisto viene comunicata all'Autorità di Vigilanza almeno 60 giorni prima della stipula del contratto.

***

In linea generale, nei confronti con la PA è espressamente fatto divieto di:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate;
2. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle;
3. porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato;
4. effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia a pubblici funzionari;
5. distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice etico, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico, o la brand image della Società. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;

6. accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto;
7. effettuare prestazioni in favore dei consulenti, dei Partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;
8. destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
9. alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;
10. elargire, promettere o dare denaro o altra utilità a giudici, arbitri, funzionari di cancelleria, periti, testimoni, ecc., ovvero a persone comunque indicate da codesti soggetti, nonché adottare comportamenti – anche a mezzo di soggetti Terzi (es. professionisti esterni) - contrari alla legge e ai presidi aziendali, per influenzare indebitamente le decisioni dell'organo giudicante ovvero le posizioni della Pubblica Amministrazione, quando questa sia una parte nel contenzioso;
11. favorire indebitamente gli interessi della Società inducendo con violenza o minaccia, o, alternativamente, con offerta di danaro o altra utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale.

Nell'ambito di ispezioni effettuate da parte delle autorità di vigilanza presso la sede della società, dovrà essere assicurata la presenza di almeno due soggetti appartenenti alla Struttura interessata dall'ispezione, fatte salve situazioni particolari delle quali dovrà essere data espressa e tempestiva comunicazione all'Organismo di vigilanza.

SEZIONE SEZIONE B – REATI SOCIETARI

Si premette che la Società, in quanto succursale di banca estera, non l'ha l'obbligo di redigere un proprio bilancio civilistico, bensì ha l'obbligo di trasmettere il "branch report" che contiene i dati e le informazioni amministrativo-contabili all'amministrazione della Casa Madre al fine di far confluire gli stessi nel bilancio consolidato di gruppo. Il branch report è predisposto dal CFO, autorizzato dal Branch Manager e certificato dal revisore.

Sebbene i reati trattati nella presente Sezione afferiscano al processo di formazione del bilancio civilistico, si è ritenuto di dover ricomprendere gli stessi nel Modello a scopo cautelativo considerando:

a) l'assimilabilità del branch report a un bilancio civilistico in quanto rappresenta la situazione economico finanziaria della Società
b) la configurabilità del Branch Manager, di fatto, in amministratore o direttore generale (autori del reato ai sensi del codice civile perché soggetti responsabili della correttezza dei dati di bilancio).

Nella lettura della presente Sezione pertanto ogni qualvolta il legislatore si riferisce al bilancio civilistico, è da intendersi nel contesto di Opel Bank Italia, il "branch report".

Considerando sin quanto qui esposto, la presente sezione è suddivisa come segue:

1. ***Reati e modalità di commissione***: contiene la descrizione delle fattispecie criminose rilevanti richiamate dall'art. 25 ter del Decreto.
2. ***Ruoli e responsabilità***; richiama i ruoli e le responsabilità interne a presidio dei rischi.
3. ***Aree sensibili e processi a rischio***; in conformità a quanto prescritto dall'art. 6 co. 2 del Decreto, illustra sinteticamente le attività a rischio nell'ambito dell'organizzazione e dell'attività aziendale e il livello di rischio associato.
4. ***Presidi interni***; descrive le responsabilità istituzionali a norma di legge, richiama i ruoli e le responsabilità organizzative interne e individua i principi di comportamento da adottarsi.

1. Reati e modalità di commissione

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

Il reato previsto dall'art. 2621 c.c. è un reato proprio: conseguentemente, per la sua configurabilità, è necessario che ad agire sia un soggetto provvisto della qualifica richiesta dalla legge, ovvero Amministratori, Direttori Generali, Sindaci e Liquidatori. E' possibile, tuttavia, che le falsità o le dolose omissioni di informazioni in bilancio e nella nota integrativa siano poste in essere dai livelli sottostanti, segnatamente dai dirigenti responsabili della redazione dei documenti contabili societari; in tal caso esse configurano reato se gli amministratori, a conoscenza delle

stesse, le abbiano deliberatamente fatte proprie. Il reato è normalmente considerato a elevato rischio intrinseco per la molteplicità delle modalità e facilità di commissione.

Fatti di lieve entità (art. 2621 bis c.c.)

Al successivo art 2621 bis, è prevista una riduzione della pena se i fatti di cui all'art. 2621 c.c. sono considerati di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità e degli effetti della condotta. La stessa riduzione della pena è prevista se i fatti di cui all'art 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'art 1[3] Regio Decreto 16 marzo 1942, n.267.

False comunicazioni sociali per le società quotate (Art. 2622 c.c.)

Il reato, applicabile alle sole società quotate, punisce i medesimi soggetti di cui sopra e il Dirigente preposto, nel caso di comunicazioni sociali dirette ai soci ed espongono consapevolmente fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti in modo concretamente idoneo ad indurre altri in errore.

Impedito controllo (art. 2625 c.c.)

Tale ipotesi di reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali qualora tale condotta abbia cagionato un danno ai soci. L'illecito può essere commesso esclusivamente dagli amministratori.

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

Tale ipotesi di reato consiste nel procedere, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli.

Soggetti attivi del reato possono essere solo gli amministratori.

Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite. Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato. Soggetti attivi del reato sono gli amministratori.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

[3] Sostituito dall'art 1 del d.lgs. n. 5/2006 con il seguente: "Non sono piccoli imprenditori gli esercenti attività commerciale in forma individuale o collettiva, che anche alternativamente:
Hanno effettuato investimenti nell'azienda per un capitale di valore superiore a euro trecentomila;
Hanno realizzato, in qualunque modo risulti, ricavi lordi calcolati sulla base della media degli ultimi tre anni, o dall'inizio dell'attività se di durata inferiore, per un ammontare complessivo annuo superiore a euro duecentomila".

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto od alla sottoscrizione di azioni o quote emesse dalla società (o dalla società controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

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

Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

Tale ipotesi di reato consiste nella violazione degli obblighi previsti dall'art. 2391, comma primo, c. c. da parte dell'amministratore di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione Europea o diffusi fra il pubblico in maniera rilevante ai sensi dell'art. 116 TUF (ovvero di altri soggetti sottoposti a vigilanza), se dalla predetta violazione siano derivati danni alla società o a terzi.

L'art. 2391, comma primo, c. c. impone agli amministratori delle società per azioni di dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata. Gli amministratori delegati devono altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale. L'amministratore delegato deve darne notizia anche alla prima assemblea utile.

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

Tale ipotesi di reato è integrata dalle seguenti condotte: a) formazione o aumento in modo fittizio del capitale sociale mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; b) sottoscrizione reciproca di azioni o quote; c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori e i soci conferenti. Si precisa che non è, invece, incriminato l'omesso controllo ed eventuale revisione da parte di amministratori e sindaci, ai sensi

dell'art. 2343, 3° comma, c.c. della valutazione dei conferimenti in natura contenuta nella relazione di stima redatta dall'esperto nominato dal Tribunale.

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

Tale ipotesi di reato consiste nella ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Soggetti attivi del reato sono esclusivamente i liquidatori.

Corruzione tra privati (2635 c.c.)

Tale ipotesi di reato rileva ai fini della responsabilità amministrativa dell'ente qualora i soggetti apicali o i soggetti subordinati diano o promettano denaro o altra utilità a:

1. amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di altre società;
2. coloro che siano sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui al punto che precede.

Si fa presente che l'ente risponderà del reato quando i predetti soggetti agiscano come corruttori, non anche quando siano stati corrotti.

La responsabilità amministrativa è limitata all'ente cui sia riconducibile il soggetto apicale o dipendente che ha posto in essere la condotta di corruzione e non riguarda invece la società cui appartiene il soggetto corrotto.

Istigazione alla corruzione tra privati (art. 2635 bis)

La fattispecie punisce chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.

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

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con atti simulati o fraudolenti, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Il reato è costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

Aggiotaggio (art. 2637 c.c.)

Tale ipotesi di reato consiste nella diffusione notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata 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.

Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638 c.c.)

Si tratta di due ipotesi di reato distinte per modalità di condotta e momento offensivo:

- la prima si realizza (i) attraverso l'esposizione nelle comunicazioni previste dalla legge alle Autorità pubbliche di Vigilanza (al fine di ostacolare l'esercizio delle funzioni di queste ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero (ii) mediante l'occultamento, con altri mezzi fraudolenti, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria. La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti od amministrati dalla società per conto di terzi;
- la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche Autorità, attuato consapevolmente e in qualsiasi forma, anche omettendo le comunicazioni dovute alle Autorità medesime.

Soggetti attivi dell'ipotesi di reato descritta sono gli amministratori, i direttori generali, i sindaci e i liquidatori.

Estensione delle qualifiche soggettive (art. 2639 c.c.)

Per tutti i reati previsti nella presente sezione, al soggetto formalmente investito della qualifica o titolare della funzione prevista dalla legge civile è equiparato sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Fuori dei casi di applicazione delle norme riguardanti i delitti dei pubblici ufficiali contro la pubblica amministrazione, le disposizioni sanzionatorie relative agli amministratori si applicano anche a coloro che sono legalmente incaricati dall'autorità giudiziaria o dall'autorità pubblica di vigilanza di amministrare la società o i beni dalla stessa posseduti o gestiti per conto di terzi.

***

In generale il rischio di commissione dei reati societari è limitato dai numerosi controlli sul budget e sulle scritture contabili che vengono periodicamente effettuati dall'Autorità di Vigilanza.

2. Aree sensibili e processi a rischio

Le aree sensibili sono stabilite specificamente dal Decreto che identifica processi e attività considerate astrattamente a rischio (bilancio, operazioni sul capitale ecc.). Tra questi:

a) coordinamento e gestione della contabilità generale, con particolare riferimento alle attività di:

- rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi, finanziari ed economici;
- corretta tenuta dei rapporti amministrativi con i terzi (es. fornitori);
- gestione amministrativa e contabile dei cespiti;
- accertamenti di tutti gli altri fatti amministrativi in corso d'anno (es. costi del personale, penalità contrattuali, ecc.);
- verifica dei dati provenienti dai sistemi alimentanti.

b) raccolta e aggregazione dei dati contabili necessari per la predisposizione del branch report

c) tenuta delle scritture contabili.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

3. Ruoli e responsabilità interne

I ruoli interni a presidio dei rischi sono:

- Branch Manager
- Director Finance
- Director Operations
- Manager Finance
- Manager Sales
- Manager Retail Acquisitions
- Manager Collections
- Manager Marketing
- Manager Insurance.

4.Presidi interni

Considerato il modello di Governance adottato, nonché le norme di legge di riferimento, i presidi interni a prevenzione dei reati sono i seguenti:

- ***il sistema di Governance in generale***
- ***le direzioni e le funzioni*** che a diverso titolo, anche istruttorio o esecutivo, intervengono nei processi e nelle attività a rischio
- ***il complesso delle regole e delle procedure interne aventi rilievo nella prevenzione dei reati***

In relazione all'ambito di manifestazione degli illeciti trattati nella presente sezione, rilevano le funzioni interne riconducibili all'area amministrativa per quanto attiene la veridicità e completezza delle informazioni fornite nel contesto delle operazioni sopra descritte.

Le funzioni richiamate collaborano attivamente con il CFO e il Branch Manager fornendo senza indugio le informazioni richieste da quest'ultimo e segnalando tempestivamente il verificarsi di anomalie o disfunzioni nel normale svolgimento delle proprie mansioni qualora lo ritengano necessario.

5. Protocolli adottati ai sensi dell'art. 6 co. 2 del decreto

5.1 False comunicazioni sociali

Ai sensi dell'art. 2381 c.c., è compito dell'organo delegato curare che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa.

►In particolare, nel caso di Opel Bank Italia, è compito del Branch Manager

- curare che i poteri negoziali e di spesa e tutte le altre attività che possono originare transazioni contabili configurino un quadro chiaro ed esaustivo in merito alle aree di competenza attribuite, congruente con l'organizzazione e con l'attività aziendale
- promulgare e sostenere il principio della corresponsabilità dei dati che confluiscono nel branch report, in relazione al quale la veridicità, correttezza e completezza delle informazioni sulla situazione economica, patrimoniale e finanziaria configura attribuzione di responsabilità oltre che della funzione amministrativa, anche nei confronti di qualunque altra funzione o di chiunque per i poteri attribuiti possa generare rilevazioni contabili, nonché di chiunque sia in possesso di informazioni necessarie alla completa e corretta rappresentazione del branch report; dal quale consegua un obbligo generale di riferire tempestivamente e periodicamente al Responsabile dell'Ufficio Amministrazione ogni notizia necessaria alla corretta rappresentazione dei dati e delle informazioni contabili ovvero, ogni notizia relativa a presumibili distorsioni informative o omissioni contabili.

►E' compito dell'Area Finance a presidio della correttezza della veridicità e completezza dei dati e delle informazioni da inserire nel branch report, un processo strutturato che, conformemente alla migliore prassi si articoli su:

- indirizzi in merito alle regole di condotta e ai comportamenti che le funzioni interessate alla formazione di bilancio devono rispettare al fine di assicurare l'informazione completa, veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società
- mappatura, definizione e regolamentazione dei processi amministrativo-contabili e delle attività rilevanti ai fini delle registrazioni e delle elaborazioni dei dati contabili nonché delle informazioni necessarie alla redazione del branch report
- attestazioni della veridicità delle poste indicate nel branch report più significative originate da altri soggetti
- pianificazione delle chiusure contabili di ciascuna funzione (personale, commerciale, ecc.) e definizione delle relative modalità.

Per la prevenzione dei reati di false comunicazioni sociali (ex art. 2621 c.c.) e false comunicazioni sociali in danno dei soci e dei creditori (ex art. 2622 c.c.), si richiede:

- la sottoscrizione da parte dei responsabili che hanno concorso alla formazione della bozza di branch report e delle altre comunicazioni sociali di una dichiarazione attestante la veridicità, la completezza e la coerenza dei dati e delle informazioni ivi contenute;
- l'invio del branch report approvato, comprensivo della relazione della società di revisione al Branch Manager e all'organismo di Vigilanza;
- la verifica, con cadenza periodica, dei saldi dei conti di contabilità generale al fine di garantire la quadratura della contabilità generale con i rispettivi partitari e con i conti sezionali;
- l'identificazione delle risorse interessate, dei dati e delle informazioni che le stesse devono fornire, nonché delle tempistiche, per la predisposizione del branch report.
- la verifica della completezza e correttezza dei dati e delle informazioni comunicate dalle suddette risorse e sigla sulla documentazione analizzata.

5.2 Controlli di legge

5.2.1 Impedito controllo della società di revisione, del collegio sindacale e dei soci

A presidio il Branch Manager adotta le seguenti iniziative cautelative:

- in caso di effettiva constatazione dell'impedimento assume le necessarie iniziative per rimuovere ogni ostacolo all'esercizio delle funzioni del soggetto deputato al controllo
- in caso di impossibilità o di motivato rifiuto di adempiere alle richieste della società di revisione, assume le opportune deliberazioni in merito comunicandole se del caso al Consiglio di Amministrazione e/o al Management della Casa Madre.

5.2.2 Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza

Il reato rileva potenzialmente nel contesto dei controlli e delle ispezioni delle diverse Autorità di Vigilanza. Poiché anche in questo caso reati possono consumarsi solo in relazione a una posizione di inerzia, a seguito di contestazione formale dei soggetti deputati al controllo il Branch Manager adotta le medesime iniziative cautelative di cui al paragrafo precedente.

5.3 Corruzione tra privati e istigazione alla corruzione

Sono considerate a rischio reato le attività di ciclo attivo e passivo, la gestione delle risorse finanziarie, la gestione e assunzione del personale interno, dei collaboratori e consulenti,nella scelta dei parner commerciali, vale a dire le attività in cui Opel Bank Italia e ha rapporti diretti con soggetti privati.

Per quanto attiene a principi di comportamento, le regole di condotta e i presidi attualmente in essere in riferimento alle fattispecie considerate, si intendono qui richiamati i concetti espressi in

occasione dell'analisi del potenziali fenomeni corruttivi effettuata in materia dei rapporti con la Pubblica Amministrazione per quanto applicabili, integrate dai principi cogenti del Codice Etico aziendale.

Nella gestione del credito al consumo potrebbe astrattamente configurarsi il reato di corruzione tra privati mediante l'omissione delle verifiche previste per l'erogazione del credito o la concessione del credito a soggetti che non possiedono i requisiti per l'ottenimento dello stesso.
A tutela si osservano i seguenti principi generali:

- tutte le scelte relative al lancio di nuovi prodotti che possono comportare un impegno per la Società nei confronti di terzi vengono condivise e autorizzate dalle Unità operative di gruppo.
- i vantaggi economici dei prodotti finanziari e assicurativi da riconoscere ai partner commerciali seguono il medesimo iter autorizzativo e sono precedute da un analisi sulla rischiosità dell'operazione.
- le operazioni di cartolarizzazione effettuate dalla Società prevedono differenti momenti di valutazione e sono oggetto di valutazione sia del Branch Manager nei limiti della delega conferita che dal Consiglio di Amministrazione della Casa Madre.
- il processo di erogazione del credito prevede il coinvolgimento di diverse funzioni della Società responsabili, ciascuna per gli ambiti di rispettiva competenza; in particolare, le attività di sviluppo commerciale sono svolte da funzioni diverse rispetto a quelle che gestiscono operativamente l'erogazione dei prodotti/servizi.
- il processo di gestione ed erogazione del credito prevede la segregazione dei controlli per ciascuna fase;
- il processo di gestione e valutazione della redditività delle relazioni commerciali con i convenzionati, relativamente ai prodotti di credito al consumo è attribuito a distinte/i funzioni/organi aziendali responsabili
- ciascuna fase rilevante connessa alla stipula e alla gestione di contratti/convenzioni con la clientela e le controparti deve risultare da apposita documentazione scritta;
- ogni accordo con i partner è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere, in ragione della tipologia di operatività e controparte;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, le funzioni che partecipano al processo sono responsabili dell'archiviazione e della conservazione della documentazione di propria competenza.

A ulteriore presidio la Società:

- organizza per le concessionarie che offrono servizi finanziari corsi di formazione sulle verifiche da svolgere e sulle informazioni da fornire al cliente finale

- monitora costantemente il rispetto delle condizioni contrattuali sia da parte dei clienti finali che da parte delle concessionarie
- ha adottato il documento ***Deleghe in materia di concessione del credito*** che definisce il sistema dei poteri vigente.

6. Presidio delle direzioni e funzioni interne

In relazione all'ambito di manifestazione degli illeciti trattati nella presente Sezione, rilevano le funzioni interne riconducibili all'Area Finance, all'Area Risk Management, all'Area Sales and Marketing, per quanto attiene la veridicità e completezza delle informazioni fornite nel contesto delle operazioni sopra descritte.

Le funzioni collaborano attivamente con la funzione di Internal Audit fornendo senza indugio le informazioni richieste da quest'ultimo e segnalando tempestivamente il verificarsi di anomalie o disfunzioni nel normale svolgimento delle proprie mansioni qualora lo ritengano necessario.

I destinatari del Modello hanno l'obbligo di:

1) tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al socio ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
2) osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
3) assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
4) effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza.

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

con riferimento al paragrafo 5.1:

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

con riferimento al precedente punto 5.2:

- restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale;

con riferimento al precedente punto 5.3:

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte del socio, del Collegio Sindacale o della società di revisione;
- porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- omettere di mantenere traccia di tutta la documentazione richiesta e consegnata agli organi di controllo, nonché di quella utilizzata nell'ambito delle attività assembleari;
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti dell'Autorità di Vigilanza, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalla predetta autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle autorità pubbliche di vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Al fine di prevenire la commissione del reato di corruzione tra privati, è fatto inoltre divieto di:

- effettuare ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a soggetti appartenenti ad enti privati;
- distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice etico, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a soggetti appartenenti ad enti privati, o a loro familiari, che possa

influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;

- accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.), in favore di soggetti appartenenti a enti privati, che possano determinare le stesse conseguenze previste al precedente punto;
- effettuare prestazioni in favore dei consulenti, dei partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere

SEZIONE C – REATI IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LAVORO

Premessa

La Sezione attinente ai reati di *omicidio colposo* e di *lesioni personali gravi o gravissime* commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro ex D. Lgs. 9 aprile 2008, n. 81 (d'ora in poi T.U.)[4] come modificato dal D. Lgs. 3 agosto 2009, n. 109 intende dare attuazione al dettato normativo dell'art. 30 del T.U. assicurando:

1) *un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:*
   a) *al rispetto degli standard tecnico strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici*
   b) *alle attività di valutazione dei rischi ecc.*
   c) *alle attività di natura organizzativa*
   d) *all'attività di sorveglianza sanitaria*
   e) *all'attività di formazione e informazione*
   f) *all'attività di vigilanza all'acquisizione di documentazione*
   g) *alle periodiche verifiche dell'applicazione delle procedure*
   h) *all'acquisizione e documentazione*
2) *un idoneo sistema di registrazione dell'avvenuta effettuazione delle attività di cui sopra*
3) *un'articolazione delle funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo dei rischi nonché un sistema disciplinare adeguato a sanzionare il mancato rispetto delle misure indicate nel Modello*

[4] Per "norme sulla tutela della salute e sicurezza sul lavoro" si intendono non solo quelle inserite nelle leggi specificatamente antinfortunistiche, ma anche tutte quelle che direttamente o indirettamente perseguono il fine di evitare incidenti sul lavoro o malattie professionali e che in genere tendono a garantire la sicurezza del lavoro in relazione all'ambiente in cui esso deve svolgersi.

4) un idoneo sistema di controllo dell'attuazione del Modello e del suo aggiornamento.

Tali precetti, la cui sostanziale applicazione configura i requisiti dell'esimente della responsabilità amministrativa d'impresa ex D. Lgs 231/01, in linea di principio non aggiungono contenuti alle misure di prevenzione vera e propria dettate dal T.U., ma le qualificano in termini di:

1) sistema organizzato di adempimento degli obblighi giuridici

2) registrazione e documentazione degli adempimenti

3) organizzazione interna

4) e in materia controllo di attuazione e aggiornamento del Modello, precetti già ampiamente precisati nel decreto.

Nella predisposizione della presente Sezione si è assunto pertanto, accedendo a una interpretazione estensiva della norma, che quanto disposto alla lettera **a)** dell'art. 30 costituisca un addendum precauzionale sia **1)** del dettato normativo "tecnico" fondato sui Principi comuni di cui al Titolo I (con particolare riferimento al Capo III Gestione della prevenzione nei luoghi di lavoro), al Titolo II (Luoghi di lavoro), al Titolo III Uso delle attrezzature di lavoro e dei DPI, al Titolo IV (Cantieri temporanei o mobili) ecc. che **2)** della normativa generale del D. Lgs. 231/01. Ciò premesso, la sezione è suddivisa come segue:

1. ***Fattispecie criminose rilevanti***: richiama i reati dell'art. 25 septies del Decreto;
2. ***Gestione della prevenzione: misure generali di tutela;*** individua i ruoli e le responsabilità a presidio dei rischi richiamate dal T.U.
3. ***Valutazione dei rischi***; descrive i presidi adottati ai sensi di quanto previsto nel T.U.
4. ***Verifiche dell'Organismo di Vigilanza***; descrive il coordinamento tra i diversi soggetti deputati al controllo.

1. Fattispecie criminose rilevanti

Le fattispecie criminose sono individuate dall'art. 25 septies del decreto 231***: "****In relazione al delitto di cui all'articolo* ***589*** *del codice penale, commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n.123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno. In relazione al delitto di cui all'articolo* ***590****, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi.*

Le richiamate norme così recitano:

Omicidio colposo (art. 589 c.p.)

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.

Lesioni personali colpose (art. 590 c.p.)

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.

Si tratta di reati di natura *colposa* e non solo *dolosa.*

Il *dolo* sussiste quando l'autore del reato agisce con volontà ed è cosciente delle conseguenze della sua azione od omissione; la *colpa* sussiste quando l'autore del reato, pur agendo con volontà, non ha in alcun modo preso coscienza delle conseguenze della sua azione a causa della ***sua negligenza, imprudenza, imperizia o inosservanza di leggi, regolamenti, ordini e discipline.***

In merito alla discussa contraddizione tra "reato commesso *nell'interesse o a vantaggio dell'ente*" quale condizione per la responsabilità dell'ente ai sensi del Decreto 231/01, e la natura *colposa* di questi reati, la dottrina e successivamente la giurisprudenza hanno sostenuto che il vantaggio dell'ente nei reati colposi va ricercato non nell'evento del reato bensì nella condotta dell'Ente, individuando nel deficit organizzativo "desumibile" dagli incidenti e sino a prova contraria la causa degli stessi e nel presunto vantaggio economico derivatone ("desumibile" risparmio nella prevenzione), il presupposto della punibilità dell'ente ai sensi del d.lgs. 231/01[5].

2. Gestione della prevenzione: misure generali di tutela

Dato atto che il Branch Manager, in qualità di datore di lavoro (DL), ha adempiuto ai doveri non delegabili dettati dall'art. 17 del TU:

1) ha elaborato, con il supporto del RSPP e del medico competente all'uopo designati, il Documento di Valutazione dei Rischi (DVR) dopo aver considerato i luoghi di lavoro aziendale, le attività svolte, le responsabilità e le pratiche inerenti, attenendosi ai precetti di cui all'art. 15 tra cui: la valutazione dei rischi, la programmazione della prevenzione, l'eliminazione dei rischi e, ove ciò non sia possibile, la loro riduzione al minimo, il rispetto dei principi ergonomici, la riduzione dei rischi alla fonte, la sostituzione di ciò che è pericoloso con ciò che non lo è, o lo è di meno, la limitazione al minimo dei lavoratori esposti al rischio, l'utilizzo limitato degli agenti nocivi, la priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale, il controllo sanitario dei lavoratori, l'allontanamento del lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione, l'informazione, la formazione e l'addestramento, la partecipazione e la consultazione dei lavoratori, le misure di emergenza, l'uso di segnaletica, la regolare manutenzione di ambienti, attrezzature e impianti.

[5] Tesi probatoria contraddetta dalla Cassazione Sez. IV n. 27735 del 16 luglio 2010 la quale ha affermato che "il d.lgs. 231/01 non delinea un'ipotesi di responsabilità oggettiva, prevedendo, al contrario, la necessità che sussista la c.d. colpa dell'organizzazione dell'ente".

2) ha inoltre designato il responsabile del servizio di prevenzione e protezione dai rischi (RSPP d'ora in poi)

Nella presente Parte sono richiamati gli obblighi dei diversi soggetti interni (con particolare riferimento a coloro che rivestono posizioni di garanzia[6]) che a diverso titolo intervengono nella gestione della prevenzione. In merito si assume che, ai sensi dell'art. 299 del TU, le posizioni di garanzia relative a datore di lavoro, dirigenti, medico competente e preposti gravano altresì su tutti coloro che, pur sprovvisti di regolare investitura, esercitino in concreto i poteri giuridici riferiti a ciascuno di tali soggetti.

Conformemente alla disciplina di riferimento, oltre al datore di lavoro, soggetti rilevanti ai fini delle misure di prevenzione e protezione per i luoghi di lavoro riconducibili alla sede aziendale di cui al punto precedente sono il Dirigente, il Responsabile del Servizio di Prevenzione e Protezione (RSPP) e gli altri addetti (ASPP), i preposti, i lavoratori incaricati della gestione delle emergenze, il rappresentante dei lavoratori per la sicurezza (RLS), il lavoratore e il medico competente.

2.1 Responsabilità del datore di lavoro, del RSPP, del preposto, dei lavoratori, del medico competente

Datore di lavoro
Doveri ex artt. 17 e 18 in materia di prevenzione
A norma dell'art.17, il datore di lavoro non può delegare le seguenti attività: a) La valutazione di tutti i rischi con al conseguente elaborazione del Documento di Valutazione dei Rischi (DVR) b) La designazione del responsabile del servizio di prevenzione e protezione dei rischi (RSPP) Tra gli altri doveri il datore di lavoro deve: 1. nominare il medico competente per l'effettuazione della sorveglianza sanitaria e per il supporto alla valutazione dei rischi 2. designare il o i responsabili del Servizio di prevenzione e protezione (RSPP) 3. designare i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e di gestione dell'emergenza; 4. nell' affidare i compiti ai lavoratori e tenere conto delle capacità e delle condizioni degli stessi in relazione alla loro salute e alla sicurezza; 5. fornire ai lavoratori necessari e idonei DPI sentito il RSPP e il medico competente 6. prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico; 7. richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, delle disposizioni aziendali in materia di sicurezza sul lavoro e di uso dei DPI messi a loro disposizione 8. inviare i lavoratori alla visita medica entro le scadenze perviste 9. adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile abbandonino il posto di lavoro o la zona pericolosa

[6] Posizione di garanzia art. 40 c. p. "Non impedire un evento che si ha l'obbligo giuridico di impedire, equivale a cagionarlo"

10. informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione
11. astenersi dal richiedere ai lavoratori di riprendere la loro attività in una situazione in cui persiste un pericolo grave e immediato
12. adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro secondo le misure previste dall'art. 43 relativamente alla gestione delle emergenze
13. munire i lavoratori della tessera di riconoscimento
14. vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansioni specifica senza i ,prescritto giudizio di idoneità
15. adempiere agli obblighi di informazione, formazione e addestramento, astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato.
16. convocare le riunioni periodiche di cui all'art.35

Responsabile del Servizio di Prevenzione e Protezione (RSPP)

Doveri ex art. 32, 33 e segg. in materia di prevenzione

Il RSPP è responsabile del monitoraggio del sistema di prevenzione e protezione in atto e dell'aggiornamento periodico del DVR, provvede all'aggiornamento dei rischi, all'individuazione e valutazione dei fattori di rischio e all'individuazione delle misure per la sicurezza sulla base della specifica conoscenza dell'organizzazione del lavoro e dell'ambiente di riferimento.

In particolare è responsabile:

- della verifica della coerenza fra il livello di rischio individuato, il grado di sicurezza dei provvedimenti tecnici organizzativi e procedurali di prevenzione adottati, la frequenza ed il livello di affidabilità dei monitoraggi esercitati;
- dell'attuazione, attraverso adeguata pianificazione temporale delle verifiche sul rispetto degli obblighi a carico dei lavoratori inerenti l'osservanza delle disposizioni e delle istruzioni impartite, l'utilizzo corretto di attrezzature, sostanze pericolose, mezzi di trasporto, dispositivi di sicurezza e di protezione, la segnalazione immediata di deficienze dei mezzi di prevenzione e protezione e di condizioni di pericolo, il divieto di rimozione o alterazione dei dispositivi di protezione e sicurezza.

Il RSPP ha inoltre i seguenti compiti e responsabilità:

a) proporre e monitorare programmi di informazione e formazione per i dipendenti ai sensi dell'art. 36 e 37 del T.U

b) organizzare la riunione annuale prevista dall'art. 35 del TU

c) verificare, in sede di sopralluogo nei luoghi di lavoro aziendale, il corretto utilizzo dei D.P.I.

d) informare il Datore di Lavoro sugli aggiornamenti di legge applicabili all'attività aziendale e proporre le integrazioni ritenute necessarie o opportune

e) supportare il Datore di lavoro e/o il suo delegato nell'adempimento dei suoi obblighi di cui all'art. 18 (valutazione e scelta delle attrezzature di lavoro, delle sostanze chimiche, dei rischi per la sicurezza e salute, ecc.).

f) formulare azioni correttive/straordinarie in presenza di rilievi emersi a seguito di controlli da parte degli organi ispettivi o a seguito di denunce di infortuni o malattie professionali.

Preposto

Doveri ex art. 19 in materia di prevenzione

A norma di legge è considerato ***preposto*** chiunque assuma nelle circostanze una posizione di preminenza tale, rispetto agli altri lavoratori, da poter impartire istruzioni e direttive sulle modalità di svolgimento del lavoro e chi conseguentemente è tenuto all'osservanza dell'attuazione delle prescritte misure di sicurezza ed al controllo del rispetto di queste da parte dei lavoratori. Il Preposto, la cui qualifica si configura di fatto in relazione alle

mansioni effettivamente svolte anche temporaneamente in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli:
a) sovrintende e vigila sull'osservanza da parte dei singoli lavoratori dei loro obblighi di legge, delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso d'inosservanza, informa i superiori diretti;
b) verifica che soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
c) richiede l'osservanza delle misure per il controllo delle situazioni di rischio;
d) fa osservare ai lavoratori i doveri che a loro competono per legge e segnala gli inadempimenti ai diretti superiori;
e) segnalare tempestivamente ai diretti superiori sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale che ogni altra condizione di pericolo si verifichi durante il lavoro ovvero delle quali venga a conoscenza sulla base delle informazioni ricevute
f) in caso di pericolo grave e immediato dà istruzioni affinché i lavoratori abbandonino il posto di lavoro o la zona pericolosa; informa tempestivamente i lavoratori sul rischio stesso e sulle disposizioni prese o da prendere in materia di protezione e si astiene, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività.
Il Preposto è soggetto alle sanzioni di cui all'art. 56 del T.U.

Lavoratori

Doveri ex art. 20 in materia di prevenzione

Nell'ambito dell'attività formativa ai dipendenti è data altresì comunicazione dei doveri che a questi spettano per legge in materia di sicurezza (art. 20 T.U.).
In particolare i lavoratori hanno il dovere di:
a) osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti ai fini della protezione collettiva ed individuale;
b) utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze e i preparati pericolosi, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
c) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
d) segnalare immediatamente al responsabile della sicurezza, al dirigente o al preposto le deficienze dei mezzi e dispositivi di cui sopra, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, comunicandone notizia al rappresentante dei lavoratori per la sicurezza;
e) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
f) non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
g) sottoporsi ai controlli sanitari previsti nei loro confronti;
h) contribuire, insieme al responsabile della sicurezza, ai dirigenti e ai preposti, 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) partecipare ai programmi di formazione e addestramento organizzati dalla società.
I lavoratori sono soggetti alle sanzioni di cui all'art. 59 del T.U.

Medico competente

Doveri ex art. 25 in materia di prevenzione

Il medico competente collabora con il datore di lavoro e con il servizio di prevenzione e protezione alla valutazione dei rischi, anche ai fini della programmazione della sorveglianza sanitaria, all'attività di formazione e informazione nei confronti dei lavoratori 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.
Egli ha l'obbligo di collaborare con il datore di lavoro anche mediante l'esauriente sottoposizione a questi dei rilievi e delle proposte in materia di valutazione dei rischi che coinvolgono le sue competenze professionali in materia sanitaria[7].
Il Medico competente attua un programma di sorveglianza sanitaria e in particolare effettua visite mediche e altri esami necessari per verificare l'idoneità dei lavoratori a svolgere una mansione specifica. La sorveglianza sanitaria comprende:
a) la visita medica preventiva intesa a constatare l'assenza di controindicazioni al lavoro cui il lavoratore è destinato al fine di valutare la sua idoneità alla mansione specifica
b) la visita medica periodica per controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica (solitamente una volta all'anno).

3. Valutazione dei rischi

Nella presente Parte sono descritti la valutazione dei rischi e gli elementi principali del Sistema di prevenzione e protezione dei lavoratori adottato dalla Societàche, insieme ai ruoli e alle responsabilità descritti nella Parte precedente, configurano lo strumento di attuazione delle misure generali finalizzate a prevenire o a limitare gli effetti degli incidenti sul lavoro.

3.1 Valutazione dei rischi e DVR

Si prende atto che il datore di lavoro, con il supporto del medico competente e del RSPP, in conformità a quanto prescritto all'art. 17 del TU, ha effettuato la valutazione dei rischi e adottato il DVR che costituisce parte integrante della presente Sezione.

3.2 Prescrizioni generali e obblighi ex art. 30

Prescrizioni generali	**Prescrizioni e responsabilità ex art. 30**
Servizio di prevenzione e protezione: ai sensi dell'art. 32 il servizio deve essere organizzato in relazione agli esiti della valutazione dei rischi e può essere affidato al RSPP assicurando che gli addetti abbiano i necessari requisiti professionali.	Il compito di verificare i requisiti di idoneità del Servizio compete al RSPP sentito il parere del medico competente. Il RSPP riferisce periodicamente anche all'OdV sui miglioramenti necessari.
Formazione, informazione e addestramento: deve riguardare quanto stabilito agli artt. 36 e 37 e rispettare i termini di durata convenuti nelle sedi deputate. L'RSPP deve seguire un percorso formativo specifico in relazione ai rischi del contesto aziendale.	Tutta la documentazione inerente deve essere conservata a cura del RSPP.
Sorveglianza sanitaria: la sorveglianza di cui all'art.41 deve essere attuata dal medico competente avente i requisiti di cui all'art. 38.	Il medico competente conserva tutta la documentazione inerente ai suoi doveri e invia periodicamente al datore di lavoro e all'OdV una sintesi dell'attività svolta. Eventuali criticità riscontrate sullo stato di salute delle

[7] Cassazione penale, sez. III, 15 gennaio 2013 n. 1856

	persone che su gravi rischi per la loro salute o incolumità di cui venga a conoscenza devono essere comunicate senza indugio al datore di lavoro.
Gestione delle emergenze: a integrazione del SPP di cui all'art.32 devono essere predisposte le misure generali di cui all'art. 43 nonché specifiche misure di primo soccorso (art.45) e prevenzione incendi (art. 46).	Le prescrizioni coincidono con quanto previsto dal T.U in materia.
Tenuta della documentazione e delle statistiche infortuni; è autorizzata la tenuta su supporto informatico***.***	La tenuta della documentazione quale a titolo esemplificativo: il DVR, i DUVRI, gli aggiornamenti relativi e le procedure di sicurezza, l'attività di formazione e informazione, le statistiche relative agli infortuni, le comunicazioni agli uffici pubblici di competenza, i verbali delle riunioni periodiche, compete al RSPP e al medico competente per quanto attiene la sorveglianza sanitaria e le visite mediche.
Riunione periodica Il datore di lavoro, direttamente o tramite il RSPP, indice almeno una volta all'anno una riunione cui partecipano: a) il datore di lavoro stesso o un suo rappresentante b) i delegati di funzione c) il responsabile del servizio di prevenzione e protezione dai rischi d) il medico competente e) il rappresentante dei lavoratori per la sicurezza	Durante la riunione sono sottoposti all'attenzione dei partecipanti: i. il DVR ii. l'andamento degli infortuni e della sorveglianza sanitaria iii. i programmi di informazione e formazione dei dirigenti, dei preposti e dei lavoratori ai fini della sicurezza e della protezione della loro salute. Nel corso della riunione possono essere individuati • codici di comportamento e buone prassi per prevenire i rischi di infortuni; • obiettivi di miglioramento della sicurezza. La riunione ha altresì luogo 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.

4. Verifiche dell'Organismo di Vigilanza

Atteso che il complesso delle misure adottate è conforme a quanto prescritto dal T.U., l'OdV monitora l'adempimento degli obblighi riportati nei paragrafi precedenti.

Al fine di realizzare gli obiettivi di prevenzione della salute e sicurezza sul lavoro i diversi soggetti coinvolti nel sistema di prevenzione c.d. di *primo livello* – il RSPP, il medico competente e tutti gli altri soggetti indicati nella Parte 3 dotati di potere impeditivo - si raccordano con l'OdV incaricato del controllo c.d. di *secondo livello*.

Devono essere fornite con immediatezza all'OdV informazioni su situazioni di riscontrata inadeguatezza e/o non effettività e/o non conformità al Modello e alle relative procedure, nonché di quelle relative alle norme generali e specifiche del T.U. affinché l'OdV possa trasmetterle all'organo dirigente che avrà il compito di convocare il SPP e, ricorrendone le condizioni, promuovere le riunioni di cui all'art. 35 co.4. Il mancato rispetto delle misure indicate nel Modello potrà essere sanzionato in via disciplinare, previa segnalazione da parte dell'OdV, al Branch Manager.

SEZIONE D- REATI DI RICETTAZIONE, RICICLAGGIO, IMPIEGO DI BENI, DENARO E UTILITA' DI PROVENIENZA ILLECITA E AUTORICICLAGGIO

Premessa

Le fonti normative antiriciclaggio sono:

- il D. Lgs. 231/07 (Decreto Antiriciclaggio), concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio indirizzato agli operatori ivi specificati della stessa specie di Opel Bank Italia;
- gli articoli del codice penale 648 (Ricettazione), 648 bis c.p. (Riciclaggio) e 648 ter (Impiego di denaro, beni o utilità di provenienza illecita), inseriti dall'articolo 63 del Decreto Antiriciclaggio tra i reati presupposto nel D.lgs. 231/01 all'articolo 25 octies.
- Circolare Banca D'Italia del 31 Dicembre 2009 sull" Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo nonche della direttiva 2006/70/CE che ne reca misure di esecuzione"
- Decreto Legislativo 22 giugno 2007, n. 109 "Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attivita' dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE"
- Provvedimento Banca d'Italia del 10/03/2011, in materia di organizzazione, procedure e controlli interni, volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'art 7 comma 2 del DLgs 231/2007.
- Provvedimento Banca d'Italia dell'11/04/2013 recante Disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231
- Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (Testo rilevante ai fini del SEE)

Tale impianto normativo è stato poi integrato dalla Legge 184/14 che ha introdotto nel codice penale e nel d. lgs. 231/01, l'art. 648 ter 1 c.p. Autoriciclaggio il quale punisce "*chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione del delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa*".

Il Legislatore ha così riconosciuto la natura plurioffensiva del fenomeno del riciclaggio, associando alla tutela giuridica del patrimonio individuale la tutela di altri due beni giuridici ritenuti altrettanto

meritevoli: l'amministrazione della giustizia nel suo complesso e la libera concorrenza (potenzialmente lesa dalle maggiori disponibilità rivenienti dai delitti sanzionati dalla nuova fattispecie di cui all'art.648 ter 1.c.p.).

Ai sensi dell'art 648 bis il riciclaggio è punibile soltanto «fuori dei casi di concorso nel reato» presupposto. Esso non colpisce quindi, né il riciclaggio compiuto autonomamente dall'autore del reato, né quello compiuto dal "riciclatore" che concorra anche nel compimento del reato stesso.

L'introduzione dell'art. 648 ter 1 c.p. ha così superato la c.d. *clausola di riserva* ex art. 649 c.p.p. "l'imputato prosciolto con sentenza irrevocabile non può essere di nuovo sottoposto a procedimento penale per il medesimo fatto" introducendo una nuova fattispecie giuridica diversa da quella contenuta nell'art 648 bis c.p., in relazione alla quale al reo originario veniva riconosciuta l'immunità relativa al reimpiego che, in ipotesi di successiva incriminazione, avrebbe comportato una duplice imputazione per il medesimo reato: la prima per la commissione del reato originario, la seconda per il riciclaggio che invece, conformemente a giurisprudenza e dottrina ampiamente consolidata, rappresenta solo un completamento del primo (reimpiego dell'illecito).

La nuova fattispecie di "Autoriciclaggio" configura la condotta di riciclaggio posta in essere dall'autore, anche in concorso, del reato presupposto.

Tutto ciò premesso la presente Sezione è articolata nei seguenti paragrafi:

1. ***Reati e modalità di commissione***; contiene la descrizione delle fattispecie criminose rilevanti richiamate dall'art. 25 octies del Decreto
2. ***Ruoli e responsabilità interne***; individua i ruoli a presidio
3. ***Principi di comportamento***; sono indicate le regole di comportamento a prevenzione dei reati.

1. Reati e modalità di commissione

Ricettazione (art. 648 c.p.)

La fattispecie punisce chi "*Fuori dei casi di concorso nel reato, 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 s'intromette nel farle acquistare, ricevere od occultare*".

La condotta incriminata è quella di acquistare, ricevere, occultare denaro o cose provenienti da delitto, ovvero «intromettersi» nel farli acquistare, ricevere od occultare. La formula normativa configura, quindi, due tipi di delitti: la ricettazione vera e propria e la cosiddetta intermediazione nella ricettazione.

Circa la prima forma, la nozione di «acquisto» sta a significare ogni attivita negoziale il cui effetto giuridico consista nel far entrare la cosa nella sfera giuridico-patrimoniale dell'agente.

La precisazione del significato del termine «ricevere» e correlata a quella del termine «acquisto», nel senso cioe che il primo finisce per ricomprendere ogni forma di

conseguimento della disponibilita della cosa proveniente da delitto differente da quella di acquisto. Si tratta, quindi, di una nozione residuale non quanto all'ampiezza, ma quanto al modo della sua determinazione concettuale.

L'«occultamento» a sua volta implica il nascondimento della cosa, anche a carattere temporaneo.

Quanto al secondo tipo di ricettazione, l'«intromissione» si realizza non soltanto con lo svolgimento dell'attivita di mediazione in senso strettamente civilistico, ma anche con qualsiasi attività di messa in contatto dell'autore del reato presupposto con un terzo possibile acquirente.

Riciclaggio (art. 648 bis c.p.)

La fattispecie di reato punisce *chi, fuori dei casi di concorso nel reato, sostituisce denaro, beni o altre utilità provenienti dai delitti di rapina aggravata, di estorsione aggravata, di sequestro di persona a scopo di estorsione o dai delitti concernenti la produzione o il traffico di sostanze stupefacenti o psicotrope, con altro denaro, altri beni o altre utilità, ovvero ostacola l'identificazione della loro provenienza dai delitti suddetti*.

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

La fattispecie di reato punisce *chi, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648 bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti dai delitti di rapina aggravata, di estorsione aggravata, di sequestro di persona a scopo di estorsione o dai delitti concernenti la produzione o il traffico di sostanze stupefacenti o psicotrope;*

Autoriciclaggio

Le condotte che impegnano la responsabilità del reo in relazione all'illecita natura dei proventi sono **1)** la sostituzione **2)** il trasferimento **3)** il loro reimpiego in determinate attività **4)** la rappresentazione contabile falsa o fittizia idonea a dissimularne il compimento. Condotte che sebbene non necessariamente artificiose in sé (non classificabili cioè nella più grave condotta di artifici e raggiri), sono caratterizzate da un comportamento decettivo, capace di rendere obiettivamente difficoltosa l'identificazione dell'origine delittuosa dei proventi illeciti.

Sono invece esenti le condotte che configurano un mero godimento personale del bene, del denaro o delle altre utilità.

Innanzitutto i flussi in entrata dovrebbero pervenire da una condotta criminosa che si realizza solo al superamento di alcuni limiti previsti dalla normativa sui reati fiscali. Pertanto, è necessario che siano superate le soglie di punibilita previste dal D.lgs. n. 74/2000, per poter determinare l'esistenza del reato presupposto. In secondo luogo è necessario che i flussi in uscita siano destinati ad attività imprenditoriali, economiche e finanziarie idonee a ostacolare l'accertamento della provenienza delittuosa.

Va, poi, considerato che – come chiarito dalle Linee guida di Confindustria – il reato di autoriciclaggio, in relazione ai proventi derivanti dall'evasione fiscale, comporta la necessità di identificare e isolare dal patrimonio aziendale del contribuente, il provento

illecito oggetto delle successive operazioni di reimpiego, sostituzione o trasferimento. In sostanza, è necessario che al compimento del reato fiscale presupposto segua un'azione in cui il provento della frode fiscale venga fisicamente "isolato" dal patrimonio del contribuente e trasferito su un conto corrente apparentemente terzo, gestito da un operatore fiduciario che agisce in un paese off-shore con una societa di diritto estero, non operativa e priva di reali finalita imprenditoriali. In tale particolare situazione è possibile ipotizzare l'esistenza del reato di autoriciclaggio. Nel caso in cui il risparmio d'imposta illegittimo o il provento del reato presupposto, resti confuso nel patrimonio del contribuente e venga reimpiegato anche in attivita economiche oggetto dell'ordinaria attivita aziendale, non si potrà rilevare la necessaria condotta idonea ad ostacolare l'identificazione delittuosa del bene.

2. Ruoli e responsabilità interne

I ruoli che concorrono a realizzare condizioni di prevenzione e identificazione delle situazioni a rischio di reato, oltre a quello dell'Organismo di Vigilanza, sono i seguenti:

- Branch Manager
- Responsabile Compliance & AML
- Risk Manager
- Director Operations
- Director Finance
- Manager Collections
- Manager Retail Acquisitions
- Manager Marketing
- Manager Insurance

Sono comunque tenuti a informare tempestivamente i diretti superiori ovvero gli organi deputati istituzionalmente al controllo tutti coloro che sono in possesso di informazioni relative al rischio di commissione di reato o alla sua avvenuta consumazione.

2.1 Presidi istituzionali di governo e di controllo

2.2 Funzione Antiriciclaggio

È stata istituita la Funzione Antiriciclaggio meglio definita dal Provvedimento della Banca d'Italia del 10 marzo 2011 (ovvero al documento aggiornato entrato in vigore il 1.1.2019) recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e finanziamento del terrorismo, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231.

Tale funzione ha il compito di verificare che le procedure aziendali adottate siano coerenti con l'obiettivo di prevenire e contrastare la violazione della normativa. In particolare la Funzione, anche con il supporto della Funzione Risk Management ha il compito di:

- identificare le norme applicabili e valutare il loro impatto sui processi e le procedure interne;
- collaborare all'individuazione degli assetti organizzativi finalizzati alla prevenzione e al contrasto dei rischi in discorso e verificare nel continuo il loro grado di efficacia;
- verificare l'idoneità dei modelli organizzativi adottati e proporre le modifiche organizzative e procedurali necessarie o opportune al fine di assicurare un adeguato presidio degli stessi rischi;
- prestare assistenza e consulenza agli organi aziendali e all'alta direzione; in caso di offerta di prodotti e servizi nuovi, la funzione effettua in via preventiva le valutazioni di competenza;
- trasmettere mensilmente le segnalazioni alla UIF
- curare, in raccordo con le altre funzioni aziendali competenti in materia di formazione, la predisposizione di un adeguato piano di formazione, finalizzato a conseguire un aggiornamento su base continuativa del personale dipendente e dei collaboratori
- predisporre flussi informativi diretti agli organi aziendali
- collaborare con le Autorità di controllo di cui al Decreto 231/2007.

Il Responsabile Antiriciclaggio, possiede i seguenti requisiti:

- assenza da responsabilità dirette di aree operative
- assenza di un rapporto di subordinazione con soggetti operanti in tali aree
- indipendenza
- autorevolezza e professionalità.

Alla Funzione sono stati altresì attribuiti gli adempimenti di cui all'art. 42 comma 4 del Decreto:

- la valutazione delle segnalazioni delle operazioni sospette pervenute
- l'eventuale trasmissione alla UIF delle segnalazioni ritenute sospette.

Il Responsabile antiriciclaggio ha tempestivamente predisposto la Procedura Antiriciclaggio prevista nelle disposizioni attuative di Vigilanza che costituisce parte integrante del presente Modello.

Al fine di attuare un monitoraggio continuo del sistema antiriciclaggio, la Funzione è tenuta a predisporre annualmente un Programma delle Verifiche annuale nel quale sono stabiliti:

- le aree di intervento;
- gli obiettivi relativi ad ogni intervento previsto nel piano;
- la frequenza degli interventi

- nell'ottica di verificare l'effettivo funzionamento del sistema antiriciclaggio e in particolare:
- l'adeguata verifica della clientela e la conservazione della documentazione rilevante;
- l'adeguato monitoraggio delle operazioni anche attraverso l'utilizzo degli indicatori di anomalia.

Per ragioni di opportunità la funzione di Compliance è stata delegata al Responsabile Antiriciclaggio. Secondo quanto previsto dal citato Provvedimento di Banca d'Italia, la Funzione ha il compito di verificare che le procedure interne siano coerenti con l'obiettivo di prevenire la violazione delle norme (leggi e regolamenti) e dell'autoregolamentazione (codici di condotta, codici etici).

I principali adempimenti che la funzione di conformità è chiamata a svolgere sono:

- l'identificazione nel continuo delle norme applicabili e la misurazione dell'impatto su processi e procedure;
- la proposta di modifiche organizzative e procedurali atta ad assicurare un adeguato presidio dei rischi di non conformità;
- la predisposizione di flussi informativi diretti agli organi aziendali e alle strutture coinvolte.

In caso di offerta di nuovi prodotti e/o servizi, la Funzione procede, in via preventiva, alle valutazioni di competenza e provvede a rilasciare il proprio consenso alla emissione dei nuovi prodotti. Nel caso si renda necessario valutare modifiche ai prodotti già esistenti con particolari complessità, la Funzione effettua e comunica le valutazioni di competenza.

Nell'esercizio delle proprie funzioni, si avvale del personale Operativo selezionato da Opel Bank Italia e dotato di specifici compiti sintetizzati nell'apposita "Procedura antiriciclaggio e antiterrorismo".

2.3 Funzione di Internal Audit

Conformemente alle indicazioni del citato Provvedimento di Vigilanza e con riferimento al principio di proporzionalità, anche in considerazione al limitato organico della società, l'Organismo di Vigilanza si coordinerà con Funzione di Audit (Inspection General di BNP Paribas).

2.4 Funzione Risk Management

Il Risk Manager (d'ora in poi RM) esercita funzioni di indirizzo, coordinamento e controllo sul complesso delle di tutte le attività svolte dalla Socità . A tal fine, il RM può avvalersi delle strutture e delle competenze della Funzione Risk Management di Gruppo.

Il RM non ha responsabilità dirette in aree operative e non è gerarchicamente dipendente da soggetti responsabili di dette aree.

Il RM è nominato o revocato come da procedure di governance interne. La nomina e l'eventuale revoca sono tempestivamente comunicate alla Banca d'Italia a cura della funzione interna delegata a tale adempimento.

La Funzione di controllo dei rischi assume i seguenti ambiti di responsabilità:

- verifica l'adeguatezza del processo di gestione dei rischi e dei limiti operativi;
- ove richiesto fornisce al Branch Manager pareri preventivi sui rischi di operazioni rilevanti, eventualmente acquisendo, il parere di altre funzioni coinvolte nel processo di gestione dei rischi;
- collabora alla definizione delle politiche di governo e del processo di gestione dei rischi, inclusa la definizione delle azioni di mitigazione dei medesimi, con riferimento ai rischi di primo e secondo pilastro, sia soggetti a misurazione (quantificabili) che a valutazione (non quantificabili);
- concorre alla definizione delle modalità con cui effettuare le prove di stress, in particolare con riferimento all'identificazione dei rischi su cui condurre prove di stress e alle metodologie da utilizzare per la conduzione delle prove di stress sui rischi identificati;
- monitora con periodicità il profilo di rischio della società, la sua evoluzione e la sua coerenza con gli obiettivi di rischio nonché il rispetto dei limiti operativi interni,
- produce, laddove necessario o richiesto, tempestivamente, idonei flussi informativi verso il Branch Manager riguardanti: l'andamento del profilo di rischio, il raggiungimento delle soglie di attenzione, delle soglie di tolleranza e dei limiti operativi interni eventualmente definiti;
- supervisiona il Processo ICAAP, coordinandosi con le altre Funzioni per i ruoli a queste affidati;
- elabora la mappa dei rischi con cadenza annuale, da utilizzare anche ai fini ICAAP sulla base delle metodologie individuate dal Comitato Rischi. La mappa viene aggiornata con provvedimento del Branch Manager ogni qualvolta intervengano cambiamenti nell'identificazione dei rischi e della relativa tassonomia a seguito di modifiche rilevanti nelle strategie aziendali, nell'assetto organizzativo, nelle linee guida normative;
- svolge il monitoraggio andamentale del credito, del rispetto dei requisiti regolamentari e dei ratios di vigilanza prudenziale, provvedendo ad analizzarne e commentarne le caratterizzazioni e le dinamiche;
- analizza i rischi dei nuovi prodotti/servizi e di quelli derivanti dall'ingresso in nuovi segmenti operativi e di mercato;
- concorre alla definizione/revisione delle metodologie e sistemi di misurazione dei rischi interagendo con la Funzione Bilancio e Segnalazioni di Vigilanza, anche sviluppando indicatori in grado di evidenziare situazioni di anomalia e per una corretta valutazione delle attività aziendali.
- svolge attività di Coordinamento del Comitato Rischi.

Il Risk Managment svolge una funzione di controllo su tutti i processi della società secondo indicazioni contenute nei diversi documenti quali il piano strategico, regolamenti/policy e delibere.

Nello svolgimento dei compiti assegnati il Risk Managment agisce libero da condizionamenti ed ha diritto ad accedere a tutti i dati aziendali compresi quelli gestiti da Società in Outsourcing.

È autorizzata a a svolgere verifiche periodiche all'interno delle aree operative ed in tali occasioni interagisce con tutte le funzioni aziendali, con il Central Risk Team e con l' Internal Audit utilizzando i relativi report sui diversi processi;

Le attività della funzione di controllo dei rischi sono tracciate ed i relativi risultati sono documentati e formalizzati, e vengono periodicamente trasmessi all'OdV.

2.5 Comitato Rischi

Il Comitato Rischi composto dai seguenti membri in carica permanente

- Branch Manager (Chairman)
- Risk Manager (Segretario)
- Direttore Finanziario (membro e Deputy Chairman)
- Direttore Operativo (membro e Deputy Chairman)
- Direttore Commerciale (membro
- Responsabile Funzione Bilancio (membro)
- Responsabile Credito Retail (membro)
- Responsabile Collection (membro)

è responsabile delle seguenti attività:

- implementare il processo ICAAP sotto la supervisione del Risk Managment, effettuando un monitoraggio sulla gestione complessiva dei rischi;
- approvare il Resoconto ICAAP;
- monitorare l'andamento dei rischi complessivi cui è esposta la Società e informare costantemente il Branch Manager,
- valutare l'adeguatezza dei presidi organizzativi a fronte dei rischi;
- proporre al Branch Manager le soluzioni per l'adeguamento del sistema di gestione e controllo dei rischi

Il Comitato Rischi svolge la propria attività sulla base della politica di gestione dei rischi della società e si riunisce almeno una volta ogni tre mesi. Ai fini della validità delle sedute, il quorum del Comitato deve essere di almeno 3 membri dei quali almeno un membro con la carica di Chairman / Deputy Chairman ed il Segretario (Risk Manager).

3. Protocolli di prevenzione

3.1 Adeguata verifica della clientela

La Società adempie agli obblighi di adeguata verifica della clientela come disposto dal Titolo II Capo I del Decreto 231/07, nei confronti di tutti i nuovi clienti e della clientela già acquisita. Detti obblighi si sostanziano:

- nell'identificare il cliente e verificare l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente
- nell'identificare l'eventuale titolare effettivo e verificarne l'identità
- nell'ottenere informazioni sullo scopo e sulla natura prevista del rapporto continuativo o della prestazione professionale
- nello svolgere un controllo costante nel corso del rapporto continuativo o della prestazione professionale

La Società, secondo quanto previsto nella normativa rilevante, osserva gli obblighi di adeguata verifica della clientela in relazione ai rapporti e alle operazioni inerenti allo svolgimento della propria attività istituzionale e, in particolare quando:

- instaura un rapporto continuativo;
- sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione di un cliente;
- vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile.

Nell'adempiere all'adeguata verifica della clientela la Società utilizza appositi moduli di acquisizione dei dati e delle informazioni relative alla clientela richiesti dalla normativa, con distinzione dei campi da valorizzare a seconda che si tratti di obblighi di adeguata verifica ordinari, semplificati o rafforzati.

Contestualmente vengono eseguiti – sempre utilizzando il sistema operativo della Società - i controlli anagrafici per escludere la presenza dei soggetti sottoposti a verifica nelle liste dei soggetti a rischio ai fini della prevenzione al terrorismo.

La documentazione acquisita viene conservata a cura della Società in formato cartaceo o elettronico per dieci anni.

L'applicazione degli obblighi di adeguata verifica della clientela, semplificati o rafforzati, avviene esclusivamente nei casi espressamente previsti e secondo le modalità indicate, rispettivamente dagli art.25, 26 e 28 del D.lgs. n.231/2007.

3.2 Segnalazioni di operazioni sospette

Ogniqualvolta i responsabili di area ravvisano delle irregolarità tali da generare la consapevolezza o il mero sospetto che le suddette abbiano dato o potrebbero dar luogo a fatti di riciclaggio, comunicano tempestivamente al Responsabile quanto rilevato.

In tal caso compete al suddetto responsabile:

- valutare le segnalazioni delle operazioni sospette pervenute

- disporre in merito all'astensione dal concludere l'operazione, in ottemperanza al disposto dell'art.23 (D. lgs. n. 231/2007) ovvero disporre in deroga ad esso nel caso ricorressero le condizioni indicate nel comma 4 della medesima norma
- trasmettere alla UIF le segnalazioni ritenute fondate, avendo cura di tutelare la riservatezza dell'identità del soggetto di primo livello responsabile della segnalazione, nonché dei clienti oggetto di segnalazione.

4. Sistema informativo verso l'OdV

Le Funzioni Antiriciclaggio, Risk Management e Comitato Rischi riportano con cadenza semestrale all'OdV le informazioni inerenti al funzionamento del sistema di prevenzione antiriciclaggio adottato dalla Società.

La comunicazione è tempestiva in caso di anomalie o eccezioni riscontrate.

SEZIONE E – DELITTI DI CRIMINALITA' INFORMATICA E TRATTAMENTO ILLECITO DEI DATI

La presente Sezione della Parte Speciale dedicata ai delitti informatici, è suddivisa nelle seguenti parti:

4. ***Reati e modalità di commissione***; contiene la descrizione delle fattispecie criminose rilevanti richiamate dall'art. 24 bis del Decreto.
5. ***Ruoli e responsabilità interne***; individua i ruoli e le responsabilità interne a presidio dei rischi.
6. ***Aree sensibili***; in conformità a quanto prescritto dall'art. 6 co. 2 del Decreto, illustra sinteticamente le attività a rischio nell'ambito dell'organizzazione.
7. ***Protocolli di prevenzione***; sono richiamate le linee guida del garante della privacy sull'utilizzo delle risorse informatiche aziendali.
8. ***Ulteriori presidi;*** sono indicate le procedure adottate nonché le specifiche misure informatiche implementate.
9. ***Flussi informativi verso l'OdV***; è descritto il flusso informativo verso l'OdV.

1. Reati e modalità di commissione

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies.c.p.)

Se il fatto di cui all'art. 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da 1 a 4 anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da 3 a 8 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a 3 anni e con la multa da 51 a 1.032 euro.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

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, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro.

La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora cancella, altera o sopprime informazioni, dati o programmi informatici altrui, è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al n. 1) del secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

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, o 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, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1. in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2. da un pubblico ufficiale o da un incaricato di un 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;

3. da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Chiunque, fuori dei 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, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

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.)

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da 3 a 8 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da 1 a 5 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Trattamento illecito di dati (art. 167 D.Lgs. 196/2003)

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Falsità nelle dichiarazioni e notificazioni al Garante (art. 168 D.Lgs. 196/2003)

Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti,

dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Inosservanza di provvedimenti del Garante (art. 170 D.Lgs. 196/2003)

Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

Indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento (articolo 55 comma 9 D.Lgs. 231/2007)

Chiunque, al fine di trarne profitto per se' o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per se' o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonchè ordini di pagamento prodotti con essi.

Frode informatica commessa con sostituzione d'identità digitale (art. 640-ter c.p. come modificato dallo stesso D.L. 93/2013);

1. All'articolo 640-ter del codice penale, sono apportate le seguenti modificazioni:

a) dopo il secondo comma, è inserito il seguente: "La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con sostituzione dell´identità digitale in danno di uno o più soggetti";

b) all'ultimo comma, dopo le parole "di cui al secondo" sono inserite le seguenti: "e terzo".

2. Ruoli e responsabilità interne

I ruoli interni a presidio dei rischi sono:

- Manager IT
- Director Compliance
- Risk Manager

3. Aree sensibili

La società risulta essere esposta al rischio di commissione dei reati descritti nello svolgimento delle seguenti attività:

- creazione, gestione e diffusione di documenti informatici;

- accesso e gestione di sistemi informatici o telematici protetti da misure di sicurezza;
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- danneggiamento di sistemi informatici o telematici di pubblica utilità
- installazione e diffusione di apparecchiature, dispositivi o programmi informatici.
- manutenzione e sviluppo dei sistemi informativi

3.1 Protocolli di prevenzione

La Società ispirandosi ai principi di necessità, correttezza e segretezza enunciati nel Codice della Privacy aggiornato dal Dlgs 101/2018 contenente disposizioni di adeguamento al Regolamento UE 679/2016 (GDPR), adotta un adeguato sistema di sicurezza informatico basato su:

- regolamentazione dei comportamenti
- formazione obbligatoria
- controllo del personale interno ed esterno

che rappresenta un valido strumento per contrastare i rischi di:

- distruzione o perdita, anche accidentale, dei dati personali oggetto del trattamento;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta.

Il Responsabile interno IT:

1) adotta idonee misure di sicurezza, di tipo organizzativo e tecnologico per garantire la disponibilità e l'integrità di sistemi informativi e di dati e per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
2) monitora il corretto impiego degli strumenti informatici, rispettando ad ogni modo, il divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente attraverso ad esempio:
   - la lettura e la registrazione sistematica dei messaggi di posta elettronica;
   - la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
   - la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
   - l'analisi occulta di computer portatili affidati in uso
3) rende consapevoli i lavoratori delle potenzialità degli strumenti e dei programmi elettronici implementati dall'azienda, attraverso un'attività di formazione che illustra:
   - i rischi che incombono sui dati,
   - le misure disponibili per prevenire eventi dannosi
   - le responsabilità che ne derivano e che viene implementata al momento dell'assunzione, in occasione di cambiamenti di mansioni e in relazione all'introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali.

4) garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
5) collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
6) comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Internet e relativi servizi

L'utilizzo di internet deve avvenire nel rispetto della legge, dei principi di etica professionale ed unicamente a fini aziendali, al solo scopo di coadiuvare l'utilizzatore nell'esercizio delle proprie mansioni e non per questioni personali.

L'uso imprudente di alcuni servizi della rete internet, ancorché nell'ambito della normale attività aziendale, può essere fonte di particolari minacce alla sicurezza dei dati e dell'immagine aziendale.

Conformemente al Codice della Privacy adeguato al Regolamento UE 679/2016 (GDPR), Opel Bank Italia adotta le seguenti misure:

1) individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
2) configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni, reputate estranee all'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
3) eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza

In relazione all'impiego di internet, ogni utente:

1) deve evitare lo scaricamento (upload e/o download) di file e/o programmi software, anche gratuiti, se non per esigenze strettamente aziendali e fatti salvi i casi di esplicita autorizzazione della Direzione;
2) non può manomettere o creare nuovi collegamenti (internet);
3) deve evitare di condividere file su internet, in quanto tale operazione significa lasciare una "porta aperta" a virus e a particolari software (spyware, key logger) che inviano, a chi li realizza, informazioni personali a insaputa dell'utente;
4) non può visualizzare, archiviare, trasmettere o scaricare materiale fraudolento, pornografico, osceno, diffamatorio, intimidatorio e/o illegale. La società e le sue rappresentanze locali non si assumono alcuna responsabilità a riguardo.

Uso del Personal Computer

L'utente è responsabile delle macchine ad esso affidate per quanto riguarda la conservazione, l'efficienza, la regolarità di funzionamento e la pulizia.

Ogni Personal Computer, in qualunque configurazione, viene consegnato all'utente dotato di tutto ciò che necessita per il corretto funzionamento sia per quanto riguarda hardware che software:

Con riferimento all'uso di personal computer, al lavoratore è vietato:

- modificare la struttura del disco fisso;
- manomettere la struttura logica (driver, schede di memoria ecc.) della macchina;
- far utilizzare i PC o darli in uso a terzi (o familiari) che non siano dipendenti della società o da questa specificatamente autorizzati;
- utilizzare software provenienti da fonti irregolari o non regolarmente acquistati;
- divulgare dati, schede o software della Società senza l'autorizzazione del proprio superiore gerarchico;
- collegarsi al sistema informatico celando la propria identità e utilizzando il nome e/o la password di un altro utente;
- installare nella rete aziendale un proprio software che non rientri nello scopo per cui il sistema informatico è stato assegnato all'utente, al fine di evitare il rallentamento o il blocco della rete informatica aziendale.

Fermo restando quanto sopra a carico di tutti i Destinatari è fatto divieto di:

1) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
2) porre in essere condotte, anche con l'ausilio di terzi, miranti ad accedere in maniera non autorizzata ai sistemi informativi utilizzati dalla Pubblica Amministrazione o a sistemi informativi altrui con l'obiettivo di:
3) acquisire abusivamente informazioni contenute nei suddetti Sistemi Informativi;
4) danneggiare, distruggere o alterare dati o programmi contenuti nei suddetti Sistemi Informativi;
5) alterare, in qualsiasi modo, il funzionamento del sistema informativo;
6) utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi.
7) formare falsamente documenti societari aventi rilevanza esterna, mediante accesso ai sistemi e alterazione dei dati;
8) distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda.
9) porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria in assenza di una specifica autorizzazione;

10) utilizzare o installare programmi diversi da quelli autorizzati;
11) aggirare o tentare di aggirare i meccanismi di sicurezza aziendali
12) lasciare il proprio Personal Computer incustodito;
13) rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
14) detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
15) entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

Nell'ambito delle attività svolte, i fornitori terzi devono rispettare i principi di comportamento e le regole indicate nella presente Parte Speciale al fine di tutelare la sicurezza dei dati ed il corretto utilizzo dei sistemi informativi aziendali.

5. Flussi informativi verso l'OdV

Ciascun utente è tenuto a segnalare al superiore gerarchico ogni violazione, tentativo o sospetto di violazione, nonché qualsiasi malfunzionamento del sistema informatico.

Il Responsabile Interno effettua i controlli nelle aree a rischio individuate e segnala tempestivamente all'OdV qualsiasi anomalia dovesse riscontrare e ogni modifica apportata al regolamento aziendale sull'utilizzo dei sistemi informativi.

La rete informatica aziendale è periodicamente sottoposta ad attività di controllo, amministrazione e back – up finalizzate alla rimozione di ogni file o applicazione ritenuti pericolosi per la sicurezza o non inerenti all'attività lavorativa sia sui PC dei lavoratori, sia sulla rete aziendale.

Il Responsabile IT può segnalare altresì periodicamente la necessità di sottoporre l'intero sistema informatico aziendale a check-up da parte di società specializzate.

SEZ. F – REATI AMBIENTALI

La sezione è suddivisa come segue:

5. ***Reati e modalità di commissione***: richiama i reati dell'art. 25 undecies del Decreto teoricamente configurabili e le possibili modalità di commissione
6. ***Ruoli e responsabilità interne***; individua i ruoli e le responsabilità organizzative interne a presidio dei rischi
7. ***Presidi in atto***; descrive i presidi in atto
8. ***Ulteriori presidi generali***; richiama le norme di comportamento e i divieti diretti a tutti i dipendenti.

1. Reati e modalità di commissione

Tra i reati ambientali di cui all'art. 25 undecies del Decreto si riportano solo quelli inerenti alla gestione dei rifiuti, teoricamente configurabili nella realtà di OF in relazione ai rifiuti speciali prodotti:

a) toner esausti

b) RAEE.

Inquinamento ambientale (art. 452 bis c.p.)

Chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Quando l'inquinamento è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata.

Disastro ambientale (art. 452 quater c.p.)

Chiunque abusivamente cagiona un disastro ambientale è punito con la reclusione da cinque a quindici anni.

Costituiscono disastro ambientale alternativamente:

1) l'alterazione irreversibile dell'equilibrio di un ecosistema;

2) l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali;

3) l'offesa alla pubblica incolumita' in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

Quando il disastro è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata.

Associazione a delinquere diretta alla commissione di reati ambientali (art. 452 octies c.p.)

La fattispecie punisce gli accordi tra tre o più persone fisiche o giuridiche diretti all'elusione di norme ambientali al fine di conseguire un ingiusto profitto o risparmio, con l'effetto di provocare inquinamento o disastro ambientale.

Delitti colposi contro l'ambiente (art. 452 quinquies c.p.)

Se taluno dei fatti di cui agli articoli 452-bis e 452-quater (inquinamento ambientale e disastro ambientale) è commesso per *colpa*, le pene previste dai medesimi articoli sono diminuite da un terzo a due terzi.

Se dalla commissione dei fatti di cui al comma precedente deriva il pericolo di inquinamento ambientale o di disastro ambientale le pene sono ulteriormente diminuite di un terzo.

Attività di gestione illecita dei rifiuti (D. Lgs. 152/06 art. 256)

Chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 è punito:

a) con la pena dell'arresto da tre mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti non pericolosi;

b) con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti pericolosi.

Chiunque realizza o gestisce una discarica non autorizzata è punito con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro.

Si applica la pena dell'arresto da uno a tre anni e dell'ammenda da euro cinquemiladuecento a euro cinquantaduemila se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi.

Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, consegue la confisca dell'area sulla quale è realizzata la discarica abusiva se di proprietà dell'autore o del compartecipe al reato, fatti salvi gli obblighi di bonifica o di ripristino dello stato dei luoghi.

Omessa bonifica dei siti (D. Lgs. 152/06 art. 257)

Chiunque cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio è punito con la pena

dell'arresto da sei mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti.
In caso di mancata effettuazione della comunicazione di cui all'articolo 242, il trasgressore è punito con la pena dell'arresto da tre mesi a un anno o con l'ammenda da mille euro a ventiseimila euro.
Si applica la pena dell'arresto da un anno a due anni e la pena dell'ammenda da cinquemiladuecento euro a cinquantaduemila euro se l'inquinamento è provocato da sostanze pericolose.

Predisposizione di certificati di analisi dei rifiuti falsi (D. Lgs. 152/06 art. 258 c. 4, secondo periodo)

Si applica la pena di cui all'articolo 483 del codice penale a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.

Attività organizzate per il traffico illecito di rifiuti (D. Lgs. 152/06 art. 260)

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 è punito con la reclusione da uno a sei anni.
Se si tratta di rifiuti ad alta radioattività si applica la pena della reclusione da tre a otto anni.

2. Ruoli e responsabilità interne

I ruoli e le responsabilità interne a presidio delle aree di rischio sono:

3. Presidi in atto

La Società adotta i seguenti presidi:

- il ritiro dei rifiuti speciali è affidato a ditte esterne autorizzate.
- in fase di definizione contrattuale si verifica il possesso di tutte le autorizzazioni del caso.

SEZIONE G – INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA

La presente Sezione è suddivisa nelle seguenti parti:

1. ***Reati e modalità di commissione***; contiene la descrizione delle fattispecie criminose rilevanti richiamate dall'art. 25 decies del Decreto
2. ***Aree a rischio***; in conformità a quanto prescritto dall'art. 6 co. 2 del Decreto, illustra sinteticamente le attività a rischio
3. ***Principi di comportamento***; sono indicate le regole di comportamento a prevenzione dei reati.

1. Reati e modalità di commissione

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

L'art. 377-bis c.p. punisce il fatto di chi induce (mediante violenza o minaccia o con l'offerta o la promessa di danaro o altra utilità) a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere dichiarazioni utilizzabili in un procedimento penale, quando tale soggetto ha la facoltà di non rispondere.

La condotta di induzione a non rendere dichiarazioni (cioè di avvalersi della facoltà di non rispondere ovvero di rendere dichiarazioni false) deve essere realizzata in modo tipico (o mediante violenza o minaccia, ovvero con l'offerta di danaro o di qualunque altra utilità).

Il soggetto passivo è necessariamente un soggetto al quale la legge attribuisca la facoltà di non rispondere: l'indagato (o l'imputato) di reato connesso o collegato (sempre che gli stessi non abbiano già assunto l'ufficio di testimone), nonché a quella ristretta categoria di testimoni (i prossimi congiunti), cui l'art. 199 c.p.p. conferisce la facoltà di astenersi dal testimoniare.

E' ipotizzabile il caso di un dipendente imputato o indagato che venga indotto a rendere false dichiarazioni (o ad astenersi dal renderle) per evitare un maggior coinvolgimento della responsabilità risarcitoria dell'ente stesso collegata al procedimento penale nel quale il dipendente è coinvolto.

2. Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate l'attività ritenuta più specificamente a rischio è la gestione dei contenziosi giudiziali e in particolare la gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

Si è attribuito a tali reati un rating di rischio basso in quanto non hanno specificità rispetto al core business di OF

Tuttavia sono indicati di seguito i principi di comportamento che, insieme a quelli declinati nel codice etico, devono essere rispettati da tutti i dipendenti.

3. Principi di comportamento

E' fatto divieto a carico di tutti i Destinatari di:

1) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
2) prendere contatti con dipendenti o terzi coinvolti in procedimenti penali, allo scopo di indurli a rendere dichiarazioni atte ad evitare l'eventuale rischio di un coinvolgimento della società;
3) porre in essere atti di minaccia o altre forme analoghe di coartazione ovvero di dare o promettere elargizioni in danaro o altre forme di utilità affinché il soggetto (dipendente o terzo) coinvolto in un procedimento penale non presti una fattiva collaborazione al fine di rendere dichiarazioni veritiere, trasparenti e correttamente rappresentative dei fatti o non esprima liberamente le proprie rappresentazioni dei fatti, esercitando la propria facoltà di non rispondere attribuita dalla legge, in virtù delle suddette forme di condizionamento.

In particolare, nel corso di procedimenti giudiziari, è fatto divieto di:

1) elargire somme di denaro ai soggetti coinvolti quali testimoni nel procedimento penale;
2) offrire omaggi e regali alle figure coinvolte come testimoni in un procedimento penale o a loro familiari, o a conferire loro qualsiasi forma di utilità che possa influenzare la testimonianza o impedirla, ostacolarla o indurre a false dichiarazioni in fase di dibattimento per assicurare un qualsivoglia vantaggio per l'azienda;
3) accordare altri vantaggi di qualsiasi natura (promesse di assunzione, promozione, ecc.) alle persone coinvolte quali testimoni in un procedimento penale, o loro familiari;
4) effettuare alle persone coinvolte quali testimoni in un procedimento penale qualsiasi tipo di pagamento in contanti o in natura.

Inoltre, la Società deve selezionare i soggetti autorizzati a interloquire con i dipendenti coinvolti in procedimenti penali e gli eventuali colloqui intercorsi devono essere verbalizzati.