

MODELLO ORGANIZZATIVO AI SENSI DEL DECRETO LEGISLATIVO

8 GIUGNO 2001, n. 231

| | |
|---|------------------------|
| <i>Aggiornamento deliberato nella riunione del Consiglio di Amministrazione</i> | <i>del: 19/12/2006</i> |
| <i>Modifiche deliberate nella riunione del Consiglio di Amministrazione</i> | <i>del: 06/06/2007</i> |
| <i>Aggiornamento deliberato nella riunione del Consiglio di Amministrazione</i> | <i>del: 12/12/2007</i> |
| <i>Modifiche deliberate nella riunione del Consiglio di Amministrazione</i> | <i>del: 16/12/2008</i> |
| <i>Modifiche deliberate nella riunione del Consiglio di Amministrazione</i> | <i>del: 01/07/2010</i> |

Indice

| | | |
|--------|--|----|
| 1 | IL DECRETO LEGISLATIVO N. 231/2001 | 5 |
| 1.1 | Quadro normativo | 5 |
| 1.2 | Tipologie di reato previste dal D.Lgs. 231/01 | 5 |
| 1.2.1 | Reati commessi nei rapporti con la Pubblica Amministrazione | 6 |
| 1.2.2 | Delitti informatici e trattamento illecito dei dati | 6 |
| 1.2.3 | Reati di falsità in monete, in carte di pubblico credito e in valori di bollo | 7 |
| 1.2.4 | Reati societari | 7 |
| 1.2.5 | Delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali | 8 |
| 1.2.6 | Delitti contro la persona e delitti contro la personalità individuale | 8 |
| 1.2.7 | Delitti di abuso di informazioni privilegiate e di manipolazione del mercato | 8 |
| 1.2.8 | Reati di omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme antinforturistiche e sulla tutela dell'igiene e della salute sul lavoro | 9 |
| 1.2.9 | Reati di riciclaggio, ricettazione, impiego di denaro, beni o utilità di provenienza illecita e reati transnazionali | 9 |
| 1.2.10 | Norme in materia ambientale | 10 |
| 2 | MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO | 10 |
| 2.1 | Obiettivi perseguiti con l'adozione del Modello | 10 |
| 2.2 | Modifiche e integrazioni del Modello | 11 |
| 2.3 | Destinatari del Modello | 11 |
| 2.4 | Individuazione dei rischi e sistema di governo delle procedure | 11 |
| 2.4.1 | Ruolo ed individuazione dei Process Owner | 11 |
| 2.5 | Aree di attività a rischio e relativi sistemi di presidio organizzativo/gestionale | 12 |
| 2.5.1 | Attività a rischio in relazione ai reati contro la Pubblica Amministrazione | 13 |
| 2.5.2 | Attività a rischio in relazione ai delitti informatici e trattamento illecito dei dati | 14 |
| 2.5.3 | Attività a rischio in relazione ai reati di falsità in monete, in carte di pubblico credito e in valori di bollo. | 16 |

| | | |
|-------|---|----|
| 2.5.4 | Attività a rischio in relazione ai reati societari | 16 |
| 2.5.5 | Attività a rischio in relazione ai delitti di terrorismo ed eversione dell'ordine democratico, ai delitti contro la persona e contro la personalità individuale | 17 |
| 2.5.6 | Attività a rischio in relazione ai reati di abuso di informazioni privilegiate e di manipolazione del mercato | 18 |
| 2.5.7 | Attività a rischio in relazione ai reati di omicidio colposo e lesioni colpose gravi o gravissime commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro | 18 |
| 2.5.8 | Attività a rischio in relazione ai reati di riciclaggio e ricettazione | 19 |
| 3 | ORGANISMO DI VIGILANZA | 19 |
| 3.1 | Natura, qualificazione, nomina e durata in carica dell'Organismo di Vigilanza | 19 |
| 3.2 | Cause di ineleggibilità, decadenza e revoca dell'Organismo di Vigilanza | 20 |
| 3.3 | Funzioni e poteri dell'Organismo di Vigilanza | 20 |
| 3.4 | Attività di reporting dell'Organismo di Vigilanza | 21 |
| 3.5 | Flussi informativi nei confronti dell'Organismo di Vigilanza | 21 |
| 3.5.1 | Segnalazioni da parte di esponenti aziendali o da parte di terzi | 21 |
| 3.5.2 | Obblighi di informativa relativi ad atti ufficiali | 22 |
| 3.5.3 | Sistema delle deleghe | 22 |
| 4 | SELEZIONE E FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO | 22 |
| 4.1 | Selezione del personale | 22 |
| 4.2 | Formazione del personale e diffusione del Modello nel contesto aziendale | 22 |
| 4.3 | Informativa a collaboratori esterni, partner e fornitori | 23 |
| 5 | SISTEMA DISCIPLINARE | 23 |
| 5.1 | Principi generali | 23 |
| 5.2 | Sanzioni per i lavoratori dipendenti | 23 |
| 5.3 | Misure nei confronti dei Dirigenti | 24 |
| 6 | ALTRE MISURE DI TUTELA IN CASO DI MANCATA OSSERVANZA DEL MODELLO | 24 |
| 6.1 | Violazione del modello da parte di Amministratori e Sindaci | 24 |
| 6.2 | Misure nei confronti di soggetti esterni | 25 |
| 7 | CODICI DI COMPORTAMENTO | 25 |

1 IL DECRETO LEGISLATIVO N. 231/2001

1.1 Quadro normativo

Il Decreto Legislativo n. 231 dal titolo *Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica*, ha introdotto nell'ordinamento italiano un regime di responsabilità amministrativa (riferibile sostanzialmente alla responsabilità penale) a carico degli enti (da intendersi come Società, associazioni, consorzi, ecc., di seguito denominati *enti* e, singolarmente, *ente*) per alcuni reati commessi, nell'interesse o a vantaggio degli stessi:

- a) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli enti medesimi;
- b) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto. Le sanzioni previste sono pecuniarie ed interdittive (quali la sospensione o revoca di licenze e concessioni, il divieto di contrattare con la Pubblica Amministrazione (PA), l'interdizione dall'esercizio dell'attività, l'esclusione o la revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi).

La responsabilità prevista dal Decreto si configura anche in relazione a reati commessi all'estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il reato.

Il D.Lgs. 231/01 prevede, all'art. 6, una forma specifica di esonero dalla responsabilità amministrativa (c.d. *esimente*) qualora l'ente sia in grado di dimostrare:

- a) di aver adottato ed efficacemente attuato, prima della commissione di eventuali fatti illeciti, modelli di organizzazione e di gestione idonei a prevenire la commissione di reati della specie di quelli verificatisi;
- b) che il compito di vigilare sul funzionamento e l'osservanza dei Modelli nonché di curare il loro aggiornamento sia stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (di seguito, *Organismo di Vigilanza* o *OdV*);
- c) che le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente i suddetti modelli di organizzazione e gestione;
- d) che non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di cui alla precedente lett. b).

1.2 Tipologie di reato previste dal D.Lgs. 231/01

Le fattispecie di reato rilevanti, in base al Decreto e successive integrazioni, al fine di configurare la responsabilità amministrativa dell'ente, possono essere comprese nelle categorie di seguito enunciate.

1.2.1 Reati commessi nei rapporti con la Pubblica Amministrazione

Si riferisce a una serie di reati commessi nei rapporti con la Pubblica Amministrazione e disciplinati dagli artt. 24 e 25, precisamente:

- indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316-ter c.p.);
- truffa in danno dello Stato o di altro ente pubblico (art. 640, 1° comma, n. 1 c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
- corruzione per un atto d'ufficio (art. 318 c.p.);
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- corruzione in atti giudiziari (art. 319-ter c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- concussione (art. 317 c.p.);
- malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.);
- corruzione di persona incaricata di un pubblico servizio (dall'art. 320 c.p.).

1.2.2 Delitti informatici e trattamento illecito dei dati

La legge 18 marzo 2008, n. 48 ~~R~~ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno ha ampliato le fattispecie di reato che possono generare la responsabilità della società. L'art. 7 del provvedimento, infatti, ha introdotto nel D.Lgs. 231/01 l'art. 24-bis per i reati di:

- a. - accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
 - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
 - diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
 - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
 - installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
 - danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
 - danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
 - danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
 - danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- b. - falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);
- c. - frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).

1.2.3 Reati di falsità in monete, in carte di pubblico credito e in valori di bollo

L'art. 6 della Legge 23 novembre 2001, n. 409, recante "Disposizioni urgenti in vista dell'introduzione dell'euro", ha inserito nel decreto l'art. 25-bis, che mira a punire il reato di falsità in monete, in carte di pubblico credito e in valori di bollo e precisamente:

- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
- alterazione di monete (art. 454 c.p.)
- spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
- spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
- falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.) e uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.) e fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo, o di carta filigranata (art. 461 c.p.).

1.2.4 Reati societari

L'art. 3 del decreto legislativo 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, nell'ambito della riforma del diritto societario ha poi introdotto l'art. 25-ter che estende il regime di responsabilità amministrativa ai seguenti reati societari:

- false comunicazioni sociali (art. 2621 c.c.)
- false comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.)
- falsità nelle relazioni o nelle comunicazioni della Società di revisione (art. 2624, commi 1 e 2, c.c.)
- impedito controllo (art. 2625, comma 2, c.c.)
- formazione fittizia del capitale (art. 2632 c.c.)
- indebita restituzione dei conferimenti (art. 2626 c.c.)
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- illecite operazioni sulle azioni o quote sociali o della Società controllante (art. 2628 c.c.)
- operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- illecita influenza sull'assemblea (art. 2636 c.c.)
- aggio (art. 2637 c.c.)
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.)
- omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.).

1.2.5 Delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali

L'art. 25-quater, introdotto dall'art. 3 della legge 14 gennaio 2003, n. 7 di ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento del terrorismo (New York, 9 dicembre 1999), opera un rinvio generale a tutte le ipotesi attuali e future di reati terroristici ed eversivi previsti dal codice penale e dalle Leggi Speciali.

La disposizione di cui all'art. 1 della L. 6 febbraio 1980, n. 15 prevede una circostanza aggravante destinata ad applicarsi a qualsiasi reato sia "commesso con finalità di terrorismo o di eversione dell'ordine democratico".

1.2.6 Delitti contro la persona e delitti contro la personalità individuale

L'ambito dei delitti contro la persona è stato introdotto con la Legge del 9/01/06 n. 7 . che ha aggiunto l'art. 25-quater.1 e riguarda il divieto delle pratiche di mutilazione genitali femminili.

L'ambito legislativo riguardante i delitti contro la personalità individuale è stato introdotto con L. 11/08/2003 n. 228 . che ha aggiunto l'art. 25-*quinquies* che richiama specifici articoli contenuti nella Sez. I, capo III, titolo XII, Libro II del codice penale:

- riduzione o mantenimento in schiavitù e servitù (art. 600 c.p.)
- tratta di persone (art. 601 c.p.)
- acquisto o alienazione di schiavi (art. 602 c.p.)
- prostituzione minorile (art. 600-*bis* c.p.)
- pornografia minorile (art. 600-*ter* c.p.)
- detenzione di materiale pornografico (art. 600-*quater* c.p.)
- iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.).

1.2.7 Delitti di abuso di informazioni privilegiate e di manipolazione del mercato

In relazione alla disciplina sul Market Abuse (Parte V Titolo I . bis, Capo II del T.U.F.), sono stati introdotti nel disposto del D.Lgs. 231/01 (art. 25-*sexies*) i reati di abuso di informazioni privilegiate (art. 184 del TUF) e di manipolazione del mercato (art. 185 del TUF).

In particolare, per abuso di informazioni privilegiate (*insider trading*) si intende il reato per il quale chiunque, essendo in possesso di informazioni non di pubblico dominio, le divulghi a terzi, o le utilizzi al fine di effettuare o indurre altri a compiere operazioni di compravendita o altre operazioni relative a strumenti finanziari. Tali informazioni permettono ai soggetti che ne facciano utilizzo una scelta basata su un'asimmetria informativa, privilegiandoli rispetto ad altri investitori operanti sul medesimo mercato.

L'ipotesi di reato di manipolazione del mercato si configura invece a carico di chiunque diffonda informazioni false o ingannevoli o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo degli strumenti finanziari.

L'articolo 187-quinquies del TUF introduce una specifica ipotesi di responsabilità amministrativa a carico degli enti per illeciti amministrativi in materia di abusi di mercato (artt. 187. bis e 187. ter del TUF) commessi nel loro interesse o a loro vantaggio da soggetti aziendali in posizioni apicali o a loro subordinati.

1.2.8 Reati di omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

La Legge n. 123/07, ha introdotto due nuove tipologie di reato-presupposto all'interno della disciplina di cui al D.Lgs. 231/01. Nel Decreto è stato infatti inserito l'art.25-septies, successivamente sostituito dall'art. 300 del D.Lgs. 81/08, che prevede l'estensione della responsabilità amministrativa dell'ente ai reati di omicidio colposo e lesioni colpose gravi o gravissime (artt. 589 e 590 del Codice Penale), commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro.

Il provvedimento legislativo, integrando il quadro delle norme di presidio in materia di salute e sicurezza dei lavoratori nei luoghi di lavoro stabilisce, come fattore di novità, la punibilità delle Società anche per i reati di natura colposa, diversamente da quanto previsto finora per i reati in ambito 231/01, che richiedevano il presupposto della sussistenza del dolo (coscienza e volontarietà dell'azione criminosa).

Le sanzioni previste nei confronti delle Società sono di tipo interdittivo e pecuniario.

1.2.9 Reati di riciclaggio, ricettazione, impiego di denaro, beni o utilità di provenienza illecita e reati transnazionali

Il D.Lgs. n. 231 del 21 novembre 2007, relativo all'attuazione della direttiva 005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca misure di esecuzione, ha introdotto nel D.Lgs 231/01 l'art.25-octies che estende l'ambito della responsabilità amministrativa per gli enti in relazione ai reati di riciclaggio (art. 648 bis c.p.), ricettazione (art 648 c.p) e impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.).

L'art. 648 del codice penale dispone che commette il reato di ricettazione chiunque, fuori dai casi di concorso nel reato, acquista, riceve od occulta, denaro o cose provenienti da un qualsiasi delitto al fine di procurare a se od ad altri un profitto.

L'art. 648-bis del codice penale dispone che, al di fuori dei casi di concorso nel reato, commette il delitto di riciclaggio chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da un delitto non colposo ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione delittuosa della loro provenienza.

L'art. 648-ter del codice penale dispone inoltre che, al di fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 (ricettazione) e 648-bis (riciclaggio), commette il delitto di impiego di denaro, beni o altre utilità di provenienza illecita chiunque impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

Inoltre, la legge n. 146/2006, ha ratificato la normativa comunitaria contro il crimine organizzato transnazionale relativamente a quei reati posti in essere da un gruppo organizzato in più di uno Stato, ovvero a quelli commessi in uno Stato singolo, da parte di una organizzazione criminale operante su base internazionale. Tale legge comprende le seguenti tipologie di reato: associazione per delinquere (art. 416 c.p.); associazione di tipo mafioso (art. 416bis c.p.); reati concernenti intralcio alla giustizia (art. 377bis e 378 c.p.); traffico di migranti (d. lgs. n. 286/98 e successive modifiche).

1.2.10 Norme in materia ambientale

Il D.Lgs. n 152 del 3.4.2006 (art.192), pur non inserendo nuove tipologie di reato in ambito D.Lgs. 231/01, opera un rinvio al sistema sanzionatorio del D.Lgs. 231 e prevede la responsabilità solidale degli amministratori o rappresentanti della persona giuridica nel caso in cui il fatto illecito costituito dal divieto di abbandono e di deposito incontrollati di rifiuti sul suolo e nel suolo sia a loro imputabile. Le sanzioni previste sono di tipo pecuniario.

2 MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

2.1 Obiettivi perseguiti con l'adozione del Modello

Scopo del Modello è la costruzione di un sistema strutturato e organico di procedure ed altri strumenti normativi contenuti nel Sistema Documentale %Procedure del Sistema di Gestione aziendale+- e di attività di controllo, volto principalmente a prevenire (controllo ex ante) la commissione dei reati previsti dal Decreto. In particolare, mediante l'individuazione delle aree di attività a rischio e la loro conseguente proceduralizzazione, il Modello si propone di:

- determinare, in tutti coloro che operano in nome e per conto di Postecom nelle aree di attività a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo a proprio carico ma anche a carico della Società;
- ribadire che tali forme di comportamento illecito sono fortemente condannate da Postecom in quanto (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) contrarie alla legge e ai principi etico - sociali cui il gruppo Poste Italiane si attiene nell'espletamento della propria missione aziendale;
- consentire alla Società, grazie a un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente per prevenire e contrastare la commissione dei reati stessi.

Punti cardine del Modello sono, oltre ai principi già indicati:

- l'individuazione delle aree di attività a rischio dell'Azienda, vale a dire le attività nel cui ambito è ipotizzabile la commissione di reati e l'evitabilità delle fasi principali che caratterizzano le singole operazioni a rischio;

- la manutenzione di adeguate procedure aziendali a presidio delle aree di attività a rischio in modo integrato con la regolamentazione dei sistemi di controllo dei processi aziendali;
- attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- attribuzione all'OdV di specifici compiti di vigilanza e di attuazione di quanto previsto nel Modello;
- la verifica dell'effettivo rispetto ed efficacia del Modello e delle relative procedure aziendali di cui sopra;
- attuazione di un adeguato sistema sanzionatorio.

2.2 Modifiche e integrazioni del Modello

Il Modello Organizzativo è approvato con apposita deliberazione del Consiglio di Amministrazione che provvede anche alle sue modifiche su proposta dell'Amministratore Delegato.

2.3 Destinatari del Modello

Sono destinatari del Modello tutti coloro che operano per il conseguimento dello scopo e degli obiettivi di Postecom S.p.A..

2.4 Individuazione dei rischi e sistema di governo delle procedure

In relazione alle singole fattispecie di reato previste dal D.Lgs. 231/01, viene effettuata l'analisi del contesto aziendale per evidenziare dove e secondo quali modalità possono potenzialmente verificarsi eventi pregiudizievoli per gli obiettivi indicati dal citato Decreto.

Tale analisi dei rischi, comprensiva dei processi sensibili rilevati nell'ambito del Modello dei processi aziendali, direttamente o indirettamente riferibile al rischio di reato, è eseguita dalla Corporate Services - Processes and Quality che la presenta all'OdV, per poter procedere da parte dell'Amministratore Delegato alle eventuali proposte di integrazione del Modello Organizzativo.

In base alle indicazioni ed alle risultanze di tale analisi, le singole Funzioni aziendali, individuate come **Process Owner**, secondo le modalità descritte nel successivo paragrafo, elaborano ed implementano le procedure aziendali relative alle aree di attività a rischio, anche ad integrazione di procedure aziendali già esistenti avvalendosi del supporto della Corporate Services - Processes and Quality.

Le procedure che compongono il Sistema Documentale "Procedure del Sistema di Gestione aziendale" sono pubblicate sulla intranet di Postecom, secondo quanto disciplinato dalla Procedura "Gestione Documenti".

2.4.1 Ruolo ed individuazione dei Process Owner

Al fine di garantire la continua efficacia del Modello, Postecom individua il **Process Owner** che rappresenta il punto di riferimento organizzativo per il complesso delle attività svolte nell'ambito dei processi sensibili afferenti le aree di attività a rischio individuate. In particolare il Process Owner:

- 1) promuove la diffusione e la conoscenza del Modello e del Codice Etico anche attraverso l'identificazione dei fabbisogni formativi e informativi;
- 2) redige o aggiorna le Procedure ed altre tipologie documentali correlate alle attività a rischio, evidenziando un adeguato sistema di controllo, e ne cura la pubblicazione nel Sistema Documentale delle Procedure del Sistema di Gestione aziendale;
- 3) assicura il rispetto delle procedure, monitorandone l'osservanza attraverso idonee modalità, che garantiscano anche il sistema di tracciabilità dell'intero processo di cui è responsabile, secondo cui ogni operazione è provvista di un adeguato supporto documentale;
- 4) propone eventuali aggiornamenti dei processi sensibili e miglioramenti al sistema di controllo interno;
- 5) redige ed invia i flussi informativi trimestrali, per le diverse aree di attività a rischio. I flussi informativi sono trasmessi all'OdV e all'Amministratore Delegato per il tramite della Segreteria Tecnica.

Sulla base dei processi sensibili individuati nell'ambito del Modello dei processi aziendali, la Funzione HR individua quali Process Owner, i responsabili pro tempore delle Funzioni aziendali operanti nelle aree di attività a rischio, tenendo conto delle responsabilità che Postecom ha formalmente assegnato. In particolare, sulla base di tali responsabilità, Human Resources individua quali Process Owner le Funzioni aziendali che:

- hanno elevata conoscenza dei processi sensibili, in termini di attività e rischi e possono assicurare un processo di formazione e attuazione delle decisioni chiaro e trasparente;
- possono favorire modalità di monitoraggio sulla funzionalità del Modello preventivo adottato, nonché gli eventuali adeguamenti necessari.

Se l'estensione del processo presidiato e la complessità delle operazioni lo richiedono, il Process Owner potrà attribuire, secondo i criteri definiti dalla Funzione Human Resources ed in coerenza con i processi e le responsabilità organizzative aziendali, parte delle proprie competenze a uno o più **Sub-Process Owner**, che saranno responsabili delle operazioni svolte relativamente alla parte di processo assegnata.

Qualora la gestione del processo, ferma restando la sua unitarietà, in considerazione di particolari esigenze aziendali prioritariamente riferibili agli acquisti di beni e servizi, preveda la delega di specifiche attività e l'attribuzione delle conseguenti responsabilità a Funzioni aziendali diverse da quella del Process Owner di riferimento, Human Resources potrà, su richiesta e d'intesa con le Funzioni interessate, provvedere a nominare distinti **Process Owner Delegati** a cui verranno affidate con responsabilità autonoma, in tutto o in parte, le competenze del Process Owner relativamente alla gestione delle attività oggetto di delega.

2.5 Aree di attività a rischio e relativi sistemi di presidio organizzativo/gestionale

Seguono, per ciascuna tipologia di reati enunciata, i risultati dell'analisi dei rischi che tenga conto dei vantaggi potenziali che Postecom potrebbe conseguire a fronte della realizzazione degli stessi.

Per tutte le aree di attività a rischio, valgono i seguenti presidi organizzativo/gestionali di carattere generale:

- Codice Etico di Poste Italiane, e Codice di comportamento Fornitori e Partner (di cui al paragrafo 7);
- Sistema dei poteri e/o delle procure (di cui al paragrafo 3.5.3);

- Procedure e strumenti normativi che regolamentano il processo in generale;
- Sistema sanzionatorio (di cui ai paragrafi 5 e 6).

Per talune tipologie di attività esposte al rischio di reato sono stati altresì evidenziati i principali presidi organizzativi/gestionale specifici.

2.5.1 Attività a rischio in relazione ai reati contro la Pubblica Amministrazione

I reati contro la Pubblica Amministrazione hanno come presupposto l'instaurazione di rapporti e/o lo svolgimento di attività concretanti una pubblica funzione o un pubblico servizio. Tenuto conto della molteplicità dei rapporti che Postecom intrattiene con Amministrazioni Pubbliche, nonché delle attività che svolge come pubblica funzione o pubblico servizio, le aree di attività ritenute più specificamente a rischio (Aree di Attività a Rischio) sono:

1. la partecipazione a procedure di gara indette da enti pubblici, italiani o stranieri, per l'affidamento di appalti, di forniture o di servizi, di concessioni, di partnership, di asset (complessi aziendali, partecipazioni, ecc.) o di altre operazioni simili, caratterizzate dal fatto di essere svolte in un contesto potenzialmente competitivo, intendendosi tale anche un contesto in cui, pur essendoci un solo concorrente in una particolare procedura, l'ente appaltante avrebbe avuto, tuttavia, la possibilità di scegliere anche altre imprese presenti sul mercato;
2. la partecipazione a procedure di negoziazione diretta per la prestazione, in favore della Pubblica Amministrazione o di altri enti pubblici, di servizi, riservati o in regime di concorrenza;
3. l'attività di selezione, negoziazione, stipula ed esecuzione dei contratti con la Pubblica Amministrazione, Enti o Società Pubbliche;
4. l'attività di selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, ivi compresi gli appalti di lavori, che, pur non prevedendo alcun contatto con la Pubblica Amministrazione, sono potenzialmente strumentali alla realizzazione di fattispecie di reato contro la stessa;
5. le attività di gestione affidate a Postecom in attuazione di convenzioni stipulate con lo Stato o con altri enti pubblici per la prestazione di servizi a carattere preminentemente pubblicistico ivi compreso l'eventuale affidamento di tali attività in outsourcing da parte di Postecom;
6. la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego;
7. la richiesta di provvedimenti amministrativi occasionali, di autorizzazioni, licenze e concessioni per lo svolgimento di attività strumentali a quelle tipiche della Società;
8. i rapporti con le Autorità Indipendenti e di Vigilanza, i rapporti con altri organismi di diritto pubblico, nonché il rilascio di informazioni alla Pubblica Amministrazione;
9. i rapporti con i pubblici ufficiali e gli incaricati di pubblico servizio relativamente agli adempimenti fiscali, tributari e previdenziali;
10. i rapporti con l'Autorità Giudiziaria, i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale;

11. i processi di selezione e assunzione del personale;
12. la gestione delle risorse finanziarie di Tesoreria.

Costituiscono situazioni di particolare attenzione nell'ambito delle suddette aree di attività a rischio:

- a) lo svolgimento delle attività di cui ai punti 1, 2, 3, 4 e 5 in aree geografiche nelle quali non risultino garantite adeguate condizioni di trasparenza;
- b) la partecipazione alle procedure di cui ai precedenti punti 1 e 5 in associazione con un Partner (es.: *joint venture*, anche in forma di ATI, RTI, consorzi, ecc.);
- c) l'assegnazione, ai fini della partecipazione alle procedure di cui ai precedenti punti 1 e 5, di uno specifico incarico di consulenza o di rappresentanza a un soggetto terzo;
- d) l'assunzione nei ruoli dirigenziali o di quadro di persone che negli ultimi cinque anni abbiano svolto funzioni di parlamentare o abbiano avuto cariche elettive in enti pubblici territoriali, oppure incarichi di governo, oppure incarichi di collaborazione di natura continuativa con le suddette cariche elettive o di Governo;
- e) con riferimento ai punti 3 e 4 la selezione del contraente, l'esecuzione del contratto ed in particolare il ricevimento dei beni e le attività di avvenuta prestazione dei servizi e di benessere al pagamento, specialmente in relazione ad acquisti di natura immateriale, tra cui:
 - consulenze direzionali, commerciali, amministrativo-legali, e le collaborazioni a progetto
 - pubblicità
 - sponsorizzazioni
 - locazioni passive
 - attività di sviluppo di software e servizi ICT

Principali presidi organizzativo/gestionali

Con riferimento alle attività sensibili ai reati nei rapporti con la Pubblica Amministrazione, Postecom, oltre ai presidi di carattere generale individuati in precedenza, che disciplinano gli aspetti etico comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, ha provveduto ad adottare specifiche procedure aziendali in relazione ai singoli processi sensibili.

Le procedure sono raccolte nel Sistema Documentale "Procedure del Sistema di Gestione aziendale" e definiscono con chiarezza i ruoli ed i compiti delle Funzioni responsabili della gestione dei rapporti con la Pubblica Amministrazione.

Tale gestione, relativamente alle operazioni comprese nei procedimenti delle aree di attività a rischio di competenza, è affidata al Process Owner. Inoltre, nel caso di attività svolte nell'ambito di un pubblico servizio, il Process Owner o l'eventuale Sub Process Owner è responsabile nei rapporti con i terzi nei singoli procedimenti da espletare.

2.5.2 Attività a rischio in relazione ai delitti informatici e trattamento illecito dei dati

In relazione alle tipologie di delitti informatici e di trattamento illecito di dati indicate al paragrafo 1.2.2, le aree di attività ritenute specificatamente a rischio, sono:

- rispetto ai reati informatici di cui al paragrafo 1.2.2 lett. a: le comunicazioni di Postecom a mezzo di canali diretti o indiretti (es.: internet, extranet, collegamenti dedicati, ecc.), nei confronti di clienti, fornitori, dipendenti, Pubblica Amministrazione, banche e aziende di servizi, tramite l'utilizzo improprio o illegale di sistemi informatici, dispositivi hardware e infrastrutture ICT aziendali;
- rispetto al reato di falsità in un documento informatico pubblico o avente efficacia probatoria di cui al paragrafo 1.2.2 lett. b: quelle relative al processo di gestione degli archivi informatici di Postecom che contengono i dati per la gestione dei rapporti con fornitori, clienti, dipendenti, attività soggette a vigilanza di autorità pubbliche in base a discipline di settore;
- rispetto al reato di frode informatica del certificatore di firma elettronica di cui al paragrafo 1.2.2 lett. c: quelle relative a:
 - processo di identificazione della persona che fa richiesta della certificazione, anche nei casi in cui tale attività è delegata a terzi;
 - processo di rilascio e pubblicazione del certificato elettronico;
 - processo di produzione dei certificati;
 - processo di sospensione e revoca del certificato digitale
 - attività di verifica della documentazione presentata dal richiedente, in merito a titoli relativi all'attività professionale o a cariche rivestite dal richiedente stesso, nel caso in cui quest'ultimo faccia esplicita richiesta che tali informazioni siano contenute nel certificato elettronico;
 - processo di gestione del registro dei certificati;
 - processo di gestione dei dati personali dei clienti del servizio di certificazione digitale

In considerazione dell'ampio spettro di aree potenzialmente a rischio, risultano sensibili tutti i processi ICT riconducibili alla sicurezza informatica ed in particolare:

- gestione della sicurezza fisica dei sistemi ICT;
- gestione della sicurezza logica, con particolare attenzione al controllo accessi a sistemi informativi e rete dati (rete aziendale, internet, extranet) e alla crittografia dei dati e/o del canale di comunicazione (ad esempio infrastrutture firewall, Reti private virtuali, ecc.);
- sviluppo e attuazione di sistemi di monitoraggio e revisione per la prevenzione e individuazione di attività non autorizzate/illecite sulla rete, sistemi e banche dati aziendali.

Principali presidi organizzativo/gestionali

Oltre ai presidi di carattere generale individuati in precedenza, che disciplinano gli aspetti etico-comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, Postecom ha previsto i seguenti specifici presidi organizzativi e gestionali in tema di sicurezza informatica:

- policy aziendali di sicurezza informatica emanate dalla Funzione Servizi di Sicurezza di Postecom e dalla Funzione Tutela Aziendale di Poste Italiane;
- funzioni aziendali preposte alla sicurezza informatica con specifici compiti e responsabilità;
- un sistema di gestione della sicurezza informatica che prevede l'attuazione di adeguate misure per garantire la sicurezza dei dati e delle informazioni e dei dispositivi hardware;
- attività di formazione e sensibilizzazione del personale sui temi specifici della sicurezza informatica
- documento programmatico sulla sicurezza (ai sensi del D.Lgs. n. 196/03).

2.5.3 Attività a rischio in relazione ai reati di falsità in monete, in carte di pubblico credito e in valori di bollo.

In relazione a ciascuna tipologia dei reati di falsità in monete, in carte di pubblico credito e in valori di bollo, non appare ravvisabile in concreto la possibilità che rappresentanti, amministratori e dipendenti di Postecom pongano in essere, autonomamente o in concorso con terzi, nell'interesse o a vantaggio di Postecom stessa, fatti di falsificazione e di alterazione di monete, di valori di bollo o di carta filigranata in uso per la fabbricazione di carte di pubblico credito.

Infatti, il rischio di commissione di tali reati nell'interesse di Postecom è oggettivamente limitato dall'appartenenza ad un Gruppo connotato da un forte ruolo istituzionale e dalle dimensioni dell'attività esercitata dalla società.

Non risulta inoltre probabile che siano commessi, nell'interesse o a vantaggio di Postecom, i reati di spendita e introduzione nello Stato di monete falsificate da parte di proprio personale nell'esercizio delle proprie funzioni, in quanto il reato è tale da procurare un vantaggio economico esclusivamente al dipendente che lo commette.

2.5.4 Attività a rischio in relazione ai reati societari

In relazione a ciascuna tipologia di reati societari descritti al paragrafo 1.2.4, può delinearsi una specifica area di attività astrattamente a rischio. Le aree di attività ritenute più specificamente a rischio in relazione a tali reati, sono considerate le seguenti:

1. redazione del bilancio, della relazione sulla gestione e di altre comunicazioni sociali;
2. operazioni societarie che possono incidere sulla integrità del capitale sociale;
3. attività soggette a vigilanza di autorità pubbliche in base alla disciplina di settore;
4. gestione delle risorse finanziarie.

Costituiscono situazioni di particolare attenzione nell'ambito delle suddette Aree di Attività a Rischio le operazioni di conferimento, fusione e scissione.

Principali presidi organizzativo/gestionali

Oltre ai presidi di carattere generale individuati in precedenza, che disciplinano gli aspetti etico - comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, Postecom ha provveduto ad identificare i seguenti specifici presidi organizzativo/gestionali in relazione alle singole tipologie di reati societari:

1. la previsione di riunioni tra rappresentanti della Società di revisione, del Collegio Sindacale e dell'OdV;
2. la vigilanza, da parte del Collegio Sindacale, sull'effettivo mantenimento dell'indipendenza da parte della Società di revisione e la comunicazione all'OdV dei criteri di scelta della Società di revisione;
3. le lettere di attestazione predisposte, da parte dei responsabili di funzione, in sede di redazione di bilancio d'esercizio e della relazione semestrale;
4. la possibilità, da parte dell'OdV di richiedere, ai responsabili delle funzioni coinvolte nei processi di formazione del bilancio, specifiche conferme in ordine all'osservanza dei principi generali di comportamento, così come delineati dal testo del Modello Organizzativo.

2.5.5 Attività a rischio in relazione ai delitti di terrorismo ed eversione dell'ordine democratico, ai delitti contro la persona e contro la personalità individuale

La commissione nell'interesse della Società o comunque a suo vantaggio, dei reati sopra considerati, appare difficilmente ravvisabile considerate oggettivamente le finalità istituzionali di Postecom.

Tuttavia, in relazione ai reati di terrorismo ed eversione dell'ordine democratico, tenuto conto della numerosità dei rapporti che la Società intrattiene quotidianamente con la propria clientela, e, soprattutto delle prescrizioni normative che individuano nel conseguimento di un interesse o vantaggio anche indiretto per l'ente, una possibile fonte di imputabilità ex D.Lgs.231/01, sono state individuate le seguenti principali e potenziali aree di attività a rischio:

1. servizi di posta elettronica che la Società può fornire a soggetti o organizzazioni correlate a frange terroristiche/eversive;
2. approvvigionamenti e sponsorizzazioni, considerati soprattutto per quanto concerne rapporti di fornitura da terzi direttamente o indirettamente correlabili ad attività o associazioni di stampo terroristiche/eversivo, o sponsorizzazioni di entità connesse a frange terroristiche/eversive.

Principali presidi organizzativo/gestionali

Oltre ai presidi di carattere generale individuati in precedenza, che disciplinano gli aspetti etico - comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, Postecom ha provveduto ad identificare i seguenti specifici presidi organizzativo/gestionali in relazione allo specifico ambito di reati di terrorismo ed eversione dell'ordine democratico:

- politiche e procedure aziendali redatte a cura della Funzione Servizi Sicurezza con particolare riguardo alle misure di sicurezza relative al controllo degli accessi fisici alle aree aziendali;
- l'espletamento di adeguate attività di verifica dei requisiti dei fornitori nell'ambito del processo acquisti di beni e servizi.

2.5.6 Attività a rischio in relazione ai reati di abuso di informazioni privilegiate e di manipolazione del mercato

Il verificarsi di reati di abuso di informazioni privilegiate e di manipolazione del mercato (c.d. ~~Market Abuse~~) appare difficilmente ravvisabile considerato oggettivamente l'ambito di operatività di Postecom.

Principali presidi organizzativo/gestionali

Stante quanto sopra, oltre ai presidi di carattere generale individuati in precedenza, Postecom non ne ritiene necessari ulteriori per la prevenzione dei reati di abuso di informazioni privilegiate e di manipolazione del mercato in quanto non appare ravvisabile in concreto la possibilità che rappresentanti, amministratori e dipendenti di Postecom pongano in essere i reati stessi.

2.5.7 Attività a rischio in relazione ai reati di omicidio colposo e lesioni colpose gravi o gravissime commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro

La L.123/2007 prevede un'estensione della responsabilità amministrativa introducendo l'art. 25-*septies*, relativo ai "reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro".

Finalità della citata Legge è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione alla recrudescenza del fenomeno degli incidenti sul lavoro ed alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.

In via preliminare, costituiscono attività a rischio sicurezza e salute sul lavoro:

- attività relative alla manutenzione e gestione dei luoghi di lavoro;
- attività lavorative con utilizzo di videoterminali;
- attività di call center;
- attività di ufficio che comportano l'utilizzo delle seguenti attrezzature (personal computer e periferiche varie, fax, telefono, taglierina, trita carte).

Principali presidi organizzativo/gestionali

Oltre ai presidi di carattere generale individuati in precedenza che disciplinano gli aspetti etico - comportamentali che devono essere osservati dai destinatari del Modello Organizzativo, Postecom adotta ulteriori presidi analoghi a quelli già previsti nel Gruppo Poste Italiane ed individua un responsabile esterno del servizio prevenzione e protezione in possesso dei requisiti previsti dall'art. 32 del D.Lgs 81/08.

La normativa in materia di sicurezza e salute sul lavoro (L. 123/07 e D.Lgs. 81/08) prevede, inoltre, che nell'ambito delle attività di approvvigionamento (comprendente delle fasi di selezione, predisposizione delle specifiche tecniche e di esecuzione del contratto), siano garantiti i requisiti minimi di sicurezza dei lavori e servizi appaltati ed introduce specifici adempimenti da porre in essere nella fase di predisposizione della documentazione di gara e di esecuzione dei successivi accordi contrattuali.

In particolare, la nuova normativa, per quanto concerne i contratti di appalto di lavori e servizi ha introdotto l'obbligo, per il committente, di redigere il Documento Unico di Valutazione dei Rischi (DUVRI) al fine di

assicurare la riduzione dei rischi di infortuni dovuti ad interferenze nello svolgimento delle attività da parte delle imprese coinvolte nell'appalto.

Pertanto rientra nelle attività a rischio:

- la definizione e l'aggiornamento tempestivo del DUVRI, da parte delle funzioni richiedenti deputate alla gestione del contratto, con il supporto del responsabile del servizio di prevenzione e protezione;
- la verifica della idoneità tecnico-professionale delle imprese appaltatrici secondo i dettami del D.Lgs. 81/08.

2.5.8 Attività a rischio in relazione ai reati di riciclaggio e ricettazione

La commissione nell'interesse della Società o comunque a suo vantaggio, dei reati oggetto del presente paragrafo, appare difficilmente ravvisabile considerate oggettivamente le attività svolte da Postecom.

Tuttavia, in relazione ai reati di riciclaggio e ricettazione, tenuto conto della numerosità dei rapporti che la Società intrattiene quotidianamente con la propria clientela, con i propri fornitori e, soprattutto delle prescrizioni normative che individuano nel conseguimento di un interesse o vantaggio anche indiretto per l'ente, una possibile fonte di imputabilità ex D.Lgs.231/01, sono state individuate le seguenti principali e potenziali aree di attività a rischio:

- compravendita di beni e servizi;
- gestione delle risorse finanziarie.

Principali presidi organizzativo/gestionali

Oltre ai presidi di carattere generale individuati in precedenza, che disciplinano gli aspetti etico - comportamentali che devono essere osservati dai destinatari del Modello Organizzativo Postecom ha provveduto ad identificare i seguenti presidi organizzativo/gestionali in relazione alle singole tipologie:

- con riferimento alla compravendita di beni e servizi, si rinvia alla specifica procedura di acquisto di merci o servizi+ed al Codice di Comportamento Fornitori e Partner, del Gruppo Poste Italiane;
- con riferimento alla gestione delle risorse finanziarie si rimanda alla specifica procedura di processi di Gestione Amministrativa+.

3 ORGANISMO DI VIGILANZA

3.1 Natura, qualificazione, nomina e durata in carica dell'Organismo di Vigilanza

L'Organismo di Vigilanza (OdV) di Postecom è composto da tre membri di comprovata esperienza e competenza esterni alla Società, i quali abbiano i requisiti di onorabilità, professionalità e indipendenza previsti per i Consiglieri di Amministrazione. Essi sono nominati dal Consiglio di Amministrazione che ne determina anche la remunerazione. L'OdV dura in carica tre anni e i suoi membri possono essere nominati nuovamente soltanto una seconda volta.

Così come indicato dal Modello Organizzativo di Poste Italiane, i componenti esterni comprendono:

- professionisti esterni;
- membri del Collegio Sindacale;
- componenti della funzione Controllo Interno o altre idonee risorse indipendenti della Capogruppo.

L'OdV è dotato di autonomi poteri di iniziativa e controllo, con adeguate risorse a disposizione in relazione all'attività da svolgere. Si avvale di una Segreteria Tecnica formata dal responsabile della Funzione Corporate Services - Processes & Quality e si dota di un proprio regolamento interno.

3.2 Cause di ineleggibilità, decadenza e revoca dell'Organismo di Vigilanza

Costituiscono cause di ineleggibilità e decadenza dei componenti dell'OdV:

- aver ricoperto funzioni di amministratore esecutivo, nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;
- aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero di applicazione della pena su richiesta (cosiddetto "patteggiamento"), in Italia o all'estero, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex d. lgs n. 231 del 2001;
- aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero di "patteggiamento" a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Costituiscono cause di revoca dei componenti dell'OdV:

- l'omessa o insufficiente vigilanza da parte dell'OdV risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della Società ai sensi del D.lgs. n. 231 del 2001 ovvero da sentenza di applicazione della pena su richiesta (c.d. patteggiamento);
- il grave inadempimento delle funzioni e/o dei poteri dell'Organismo di Vigilanza.

La revoca è disposta con delibera del Consiglio di Amministrazione approvata con il voto dei due terzi dei presenti.

In caso di decadenza o revoca di uno di uno dei componenti dell'OdV, il Consiglio di Amministrazione provvede tempestivamente alla sua sostituzione.

3.3 Funzioni e poteri dell'Organismo di Vigilanza

Il compito di vigilare sul funzionamento e l'osservanza del Modello Organizzativo è svolto dall'OdV anche attraverso l'esame di tutti i rapporti di auditing redatti dalla Funzione Corporate Services - Processes and Quality nella materia riguardante il D.Lgs. 231/01, la quale provvede a trasmetterglieli ogni volta che l'OdV stesso ne faccia richiesta.

Il compito di curare l'aggiornamento del Modello Organizzativo in relazione all'evolversi della struttura organizzativa e a necessità sopravvenute, è svolto dall'OdV mediante proposte motivate all'Amministratore Delegato, il quale provvede a sottoporle all'approvazione del Consiglio di Amministrazione.

Ai fini dei precedenti capoversi, l'Amministratore Delegato dispone affinché l'OdV abbia accesso alle procedure aziendali ogni volta che esse vengono emanate e la Segreteria Tecnica trasmette all'Organismo di Vigilanza le delibere di delega delle attribuzioni del Consiglio di Amministrazione a suoi componenti, nonché le deleghe che detti Amministratori conferiscono al personale dipendente.

In relazione alle aree di attività sensibili di cui al precedente punto 2.5, l'OdV predispose un Piano Annuale di verifiche finalizzate a valutare l'effettiva applicazione, l'adeguatezza e la funzionalità delle procedure in termini di presidi atti a prevenire la commissione dei reati previsti dall'impianto normativo.

Tale programma di verifiche è suscettibile di variazioni sulla base di eventuali richieste di intervento da parte dell'Organismo di Vigilanza ed a fronte di criticità emerse nel corso dell'attività di analisi dei flussi o delle segnalazioni.

Quando lo ritiene opportuno, l'OdV si avvale anche di professionisti esterni per l'accertamento di fatti che sono potenzialmente idonei a costituire violazione del Modello Organizzativo, dandone preventiva informazione al Presidente e all'Amministratore Delegato.

3.4 Attività di reporting dell'Organismo di Vigilanza

In relazione allo svolgimento delle funzioni di controllo l'OdV di Postecom tiene due linee di *reporting*:

- la prima, su base continuativa, direttamente nei confronti dell'Amministratore Delegato e, con cadenza almeno semestrale, nei confronti del Presidente del Consiglio di Amministrazione;
- la seconda, su base periodica annuale, nei confronti dell'intero Consiglio di Amministrazione e del Collegio Sindacale, contenente tra l'altro un report sull'attuazione del Modello.

La presenza dei suddetti rapporti di carattere funzionale con organismi di vertice composti anche da soggetti privi di compiti operativi e, quindi, svincolati da attività gestionali e funzionali piuttosto a una attività di supervisione, costituisce un fattore in grado di conferire maggiori garanzie di indipendenza all'operato dell'OdV e un seguito più efficace all'attività di controllo di questo.

L'OdV di Postecom potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione e dal Collegio Sindacale e può chiedere di essere ascoltato dai suddetti organi, per riferire in merito al funzionamento e all'osservanza del Modello o a situazioni specifiche.

3.5 Flussi informativi nei confronti dell'Organismo di Vigilanza

3.5.1 Segnalazioni da parte di esponenti aziendali o da parte di terzi

Tutti coloro che operano per il conseguimento dello scopo e degli obiettivi della Società sono tenuti ad informare l'OdV delle possibili violazioni e/o dei comportamenti non conformi a quanto stabilito dal Modello Organizzativo. A tal fine è prevista l'istituzione di canali dedicati. Al momento, avvalendosi l'OdV del supporto della Segreteria Tecnica di Postecom, le comunicazioni possono essere inviate elettronicamente all'indirizzo segnalazioni231@postecom.it.

Sarà cura della Segreteria Tecnica trasmettere tempestivamente le comunicazioni ai componenti dell'OdV. Quando ritiene di procedere all'accertamento dei fatti, l'OdV si avvale della Segreteria Tecnica di Postecom.

3.5.2 Obblighi di informativa relativi ad atti ufficiali

Gli atti ufficiali e la reportistica riguardanti qualsiasi fattispecie che possa essere riferita alle aree di reato di cui al D.lgs. 231/01, devono essere tempestivamente trasmessi dalle funzioni aziendali di competenza all'Organismo di Vigilanza, con opportuna informativa all'Amministratore Delegato e alla Segreteria Tecnica.

3.5.3 Sistema delle deleghe

All'OdV di Postecom, infine, deve essere tempestivamente comunicato, a cura della Segreteria Tecnica di Postecom, ogni eventuale informazione in ordine ai poteri e/o alle procure, conferiti da parte del CdA o dell'AD, per singoli atti o categorie di atti.

4 SELEZIONE E FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO

4.1 Selezione del personale

La Funzione HR istituisce uno specifico sistema di valutazione del personale in fase di selezione ispirato a criteri di imparzialità, merito e professionalità, che tenga altresì conto delle esigenze aziendali in relazione all'applicazione del Decreto.

4.2 Formazione del personale e diffusione del Modello nel contesto aziendale

La formazione del personale finalizzata all'attuazione del Modello ed alla sua diffusione nel contesto aziendale è gestita dalla funzione Corporate Services - Processes and Quality ed è articolata e differenziata, tenendo conto delle diverse aree di rischio e del personale che vi opera, secondo la segmentazione di seguito indicata:

- 1) *Top Management* e *Process Owner*: vengono organizzate conferenze di sensibilizzazione e aggiornamento rispetto a tutti i temi connessi con le previsioni del D.Lgs. n. 231/2001. In particolare, tali conferenze vengono periodicamente realizzate per condividere le evoluzioni del Modello e le variazioni delle responsabilità connesse alle singole procedure, facenti parte del Sistema Documentale "Procedure del Sistema di Gestione aziendale", individuate in coerenza con il citato Decreto;
- 2) *tutti i dipendenti* che, in relazione alla specifica attività lavorativa svolta, sono coinvolti nella corretta applicazione delle procedure definite dalla Società; la formazione, prevede:
 - una parte generale dedicata alle logiche del decreto e comune a tutti i destinatari;

- una parte specifica, da progettare ed erogare esclusivamente su richiesta dei singoli Process Owner, dedicata ai processi ed alle procedure la cui applicazione è condivisa da singoli sottoinsiemi di destinatari individuati in relazione all'omogeneità delle tipologie di attività svolta.

È altresì previsto un processo di comunicazione a cascata, da parte dei Process Owner verso tutti i loro collaboratori coinvolti nella gestione/esecuzione delle singole procedure e degli altri strumenti normativi definiti all'interno del Sistema Documentale e delle Procedure del Sistema di Gestione aziendale.

- 3) *Risorse neoassunte*: ricevono, contestualmente all'assunzione, il Codice Etico del Gruppo Poste Italiane ed eventuali ulteriori informative sul tema in oggetto, anche attraverso la lettera di assunzione e/o il portale intranet aziendale
- 4) *tutto il personale*: è prevista una specifica nota informativa sulle previsioni del Decreto. Inoltre, viene favorito l'accesso - il più capillare possibile - alla sezione dedicata al Modello all'interno del Sistema Documentale e delle Procedure del Sistema di Gestione aziendale.

Inoltre, Corporate Services - Processes and Quality valuta, costantemente, gli eventuali bisogni formativi che derivino da esigenze di aggiornamento in relazione al mutare del Modello e/o di ogni altro aspetto rilevante connesso alla disciplina legislativa sul tema in argomento.

4.3 Informativa a collaboratori esterni, partner e fornitori

I soggetti esterni che intrattengono rapporti contrattuali di qualsiasi natura con la Società vengono informati che Postecom si è dotata di un Modello Organizzativo e di specifiche procedure in tema di 231, nonché di un Codice di comportamento rivolto ai Fornitori e Partner.

5 SISTEMA DISCIPLINARE

5.1 Principi generali

Aspetto essenziale per l'effettività del Modello è la predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni del Modello stesso e delle sue procedure interne disposte ai fini della prevenzione dei reati di cui al Decreto 231/2001.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte da Postecom in piena autonomia, indipendentemente dalle conseguenze penalistiche che eventuali condotte possano determinare.

5.2 Sanzioni per i lavoratori dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel Modello, sono definiti come illeciti disciplinari.

Con riferimento alle sanzioni irrogabili nei riguardi di detti lavoratori dipendenti, esse rientrano tra quelle previste dal Sistema Disciplinare aziendale, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei Lavoratori e di eventuali normative speciali applicabili.

Il Sistema Disciplinare aziendale di Postecom è costituito dalle norme pattizie di cui al Contratto Collettivo Nazionale di Lavoro (CCNL - v. art. 54 ~~in~~ ~~vece~~ ~~del~~ ~~poteri~~ ~~del~~ ~~dipendente~~; art. 55 ~~dei~~ ~~provvedimenti~~ ~~disciplinari~~; art. 56 ~~del~~ ~~codice~~ ~~disciplinare~~). In particolare, il Codice disciplinare di cui all'art. 56 del CCNL descrive i comportamenti sanzionati, a seconda del rilievo che assumono le singole fattispecie considerate, e le sanzioni in concreto previste per la commissione dei fatti stessi in base alla loro gravità.

In relazione a quanto sopra, il Modello fa riferimento alle sanzioni e alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente nell'ambito del CCNL.

Le mancanze non specificamente previste, vengono sanzionate con i ~~provvedimenti~~ ~~disciplinari~~ indicati nell'art. 55 del CCNL, facendosi riferimento, quanto all'individuazione dei fatti sanzionabili, ai ~~poteri~~ ~~del~~ ~~dipendente~~ di cui all'art. 54 e, quanto al tipo e alla misura delle sanzioni, ai principi desumibili dai criteri di correlazione.

Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti delle rispettive competenze.

Ai lavoratori viene data diffusa informazione circa il Modello Organizzativo.

5.3 Misure nei confronti dei Dirigenti

In caso di violazione, da parte di Dirigenti, delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività nelle aree a rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti Industriali.

6 ALTRE MISURE DI TUTELA IN CASO DI MANCATA OSSERVANZA DEL MODELLO

6.1 Violazione del modello da parte di Amministratori e Sindaci

La violazione del Modello da parte di Amministratori e Sindaci della Società va denunciata senza indugio all'OdV dalla persona che la rileva. Se la denuncia non è manifestamente infondata, l'OdV ne informa il Presidente del Consiglio di Amministrazione e il Presidente del Collegio Sindacale i quali provvedono a investire della questione gli organi da essi presieduti. Si applicano gli articoli 2392 e 2407 del codice civile.

6.2 Misure nei confronti di soggetti esterni

La violazione da parte di Collaboratori esterni alla Società, di Soci in Società ed enti partecipati dalla Società, di Fornitori di beni e servizi e Partner, delle norme previste dal D. Lgs. 231/01 e/o del Codice di comportamento Fornitori e Partner può essere causa di risoluzione del contratto. Tale circostanza è esplicitamente contenuta in ciascun contratto in cui la Società sia parte. La violazione va denunciata senza indugio all'Amministratore Delegato da chi la rileva. Se l'Amministratore Delegato ritiene che la denuncia sia fondata, ordina l'immediata risoluzione del contratto e ne dà notizia all'OdV. Egli dà ugualmente notizia all'OdV dei casi in cui egli non proceda a risolvere il contratto perché ritiene non fondata la denuncia o perché la risoluzione sarebbe di grave danno per la Società. La risoluzione del contratto comporta l'accertamento dei danni che la Società abbia eventualmente subito e la conseguente azione di risarcimento.

7 CODICI DI COMPORTAMENTO

Nel Codice Etico di Poste Italiane, diffuso a tutti i dipendenti della Società, sono fissati i principi guida e le direttive fondamentali a cui devono conformarsi le attività ed i comportamenti delle persone alle quali il Codice stesso è destinato.

Tale iniziativa è stata integrata dall'adozione del Codice di comportamento Fornitori e Partner che, in base a quanto stabilito dalle norme di legge e dai regolamenti interni, indica le regole di comportamento che i Fornitori e i Partner sono tenuti ad osservare specificamente nell'ambito delle attività oggetto di contratto, nonché il relativo sistema sanzionatorio, in caso di violazione dello stesso.

I Codici di comportamento, ai sensi del Decreto Legislativo 231/01 implementano i principi cardine del Modello Organizzativo attraverso un sistema di regole finalizzate a prevenire la commissione dei reati previsti dal citato Decreto.

Tali codici sono di riferimento per tutte le specifiche politiche e procedure aziendali che disciplinano le attività potenzialmente esposte ai rischi di reato.