SMARTEST

Modello organizzativo
ex D.Lgs. 231/2001

1 Parte generale

1.1 La responsabilità amministrativa

Il Decreto Legislativo 8 giugno 2001 n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa a carico delle società e degli altri enti per specifiche tipologie di reato commesse da persone fisiche che fanno parte dell'organizzazione dell'ente.

Tale nuova forma di responsabilità, sebbene sia definita amministrativa dal legislatore, presenta i caratteri propri della responsabilità penale, essendo rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare, ed essendo estese alle società le medesime cautele e garanzie del processo penale.

Questa responsabilità si aggiunge a quella della persona fisica che ha commesso materialmente il reato o il fatto illecito.

Affinché si ravvisi la responsabilità amministrativa degli enti, i reati devono essere commessi nell'interesse o a vantaggio dell'ente da persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli enti stessi (soggetti in posizioni apicali), ovvero da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati, nonché da soggetti che agiscono in nome o per conto dell'ente (soggetti sottoposti all'altrui direzione).

L'ente non risponde se i reati sono stati commessi nell'interesse esclusivo delle persone che hanno agito o nell'interesse di terzi.

La responsabilità dell'ente si configura qualora:

a) il fatto illecito sia stato commesso nell'interesse dell'ente, ovvero per favorire l'ente, indipendentemente dalla circostanza che tale obiettivo sia stato conseguito;

ovvero

b) il fatto illecito abbia portato un vantaggio all'ente a prescindere dall'intenzione di chi l'ha commesso.

1.2 Le fattispecie di reato

Quanto alla tipologia di reati che comportano il regime di responsabilità amministrativa a carico degli enti, il Decreto è in continua evoluzione e nel suo ambito sono stati introdotti, nel corso degli anni trascorsi dalla sua entrata in vigore, diverse tipologie di reato. Le fattispecie di reati attualmente rilevanti sono:

ELENCO DEI REATI PRESUPPOSTO - Ultimo aggiornamento L. 9/1/2019 n. 3, art. 1, comma 9			
Qui di seguito viene riportato l'elenco dei reati presupposto di cui si fornirà un quadro sintetico			
LEGGE	**D.Lgs 231/01**	**TIPOLOGIA DI REATO ex. D.Lgs 231/2011**	**ENTRATA IN VIGORE**
D.Lgs 231/01	Art. 24	Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico	In vigore dal 4 luglio 2001
L. 48/2008	Art. 24-bis	Delitti informatici e trattamento illecito di dati Modifica comma 1 disposta dal DL 93/2013, art 9 con l'inserimento dei seguenti reati -Trattamento illecito dei dati - Falsità nelle dichiarazioni del Garante - Inosservanza di provvedimenti del Garante	In vigore dal 5 aprile 2008 In vigore dal 17 agosto 2013 La legge 119/2013 di conversione del DL in vigore dal 16/10/2013 non ha confermato la modifica
L. 94/2009	Art. 24-ter	Delitti di criminalità organizzata (scambio elettorale politico mafioso art 416-ter c.p.)	In vigore dall'8 agosto 2009 L. 17/4/2014, n. 62
D.Lgs 231/01	Art. 25	Concussione, induzione indebita a dare promettere utilità e corruzione Introduzione fra i reati presupposto contro la pubblica amministrazione dell'art. 346 bis del codice penale rubricato "traffico di influenze illecite"	In vigore dal 4 luglio 2001 Rubrica modificata dalla L. 6/11/2012, n. 190, c. 77 lett. a) Articolo modificato (comma 1) dalla legge 9/1/2019, art. 1, comma 9, lett. b), n. 2 In vigore dal 31/1/2019 (3)
D.Lgs 350/01	Art. 25-bis	Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (2)	In vigore dal 15 agosto 2009

L. 99/2009	Art. 25-bis. 1	Delitti contro l'industria e il commercio	In vigore dal 15 agosto 2009
L. 61/2002 D.Lgs. 35/2017	Art. 25-ter	Reati societari (abrogazione artt. 2623 e 2624 c.c. modifiche art. 2625 c.c.) Modifica e/o inserimento degli artt. 2621, 2621-bis, 2621-ter e 2622 c.c. in tema di falso in bilancio, configurando il reato come delitto e inasprendo il trattamento sanzionatorio Sostituzione lett. S-bis - Delitto di corruzione fra privati (Dlgs 15/3/2017, n. 38) - GU 30/3/3017	In vigore dal 16 aprile 2002 Modificato: L. 28/12/2005, n.262 e L. 6/11/2012, n. 190, c. 77 lett. b) Falso in bilancio - modifica degli artt dal 2621 al 2642 L. n. 69 del 27/5/2015 entrata in vigore dal 14/6/2015 In vigore dal 14/4/2017
L. 7/2003	Art. 25-quater	Delitti con finalità di terrorismo o di eversione dell'ordine democratico	In vigore dal 28 gennaio 2003
L. 7/2006	Art.25-quater-1	Pratiche di mutilazione degli organi genitali femminili	In vigore dal 2 febbraio 2006
L. 228/2003	Art. 25-quinquies	Delitti contro la personalità individuale	In vigore dal 2 marzo 2006 Modificato L.6/2/2006, n.38
L. 62/2005 e seguenti	Art. 25-sexies	Abusi di mercato	In vigore dal 12 maggio 2005
L. 123/2007 e successive modificazioni	Art. 25-septies	Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro	In vigore dal 25 agosto 2007
D.Lgs 231/2007	Art. 25-octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (1)	In vigore dal 29 dicembre 2007 Modificato: L. 15/12/2014, n.186, art. 3, c. 5, lett. a) e b), con effetto dall'1/1/2015 (1)
L. 116/2009	Art. 25-novies	Delitti in materia di violazione del diritto d'autore	In vigore dal 15 agosto 2009
L. 116/2009	Art.25-decies	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci alla autorità giudiziaria	In vigore dal 15 agosto 2009
D.Lgs 121/2011	Art. 25-undecies	Reati ambientali Delitti contro l'ambiente	In vigore dal 16 agosto 2011 La legge n. 68 del 22/5/2015 entrta in vigore dal 29/5/2015 aggiunge il Titolo VI bis al c.p. dedicato ai delitti contro l'ambiente
D.Lgs 109/2011 L. 161/2017	Art. 25-duodecies	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (immigrazioni clandestine) – Nuove fattispecie - art. 30, comma 4 L. 17/10/2017, n. 161	In vigore dal 9 agosto 2012 In vigore dal 19/11/2017

L. 167/2017	Art. 25-terdecies	Inserimento nuovo articolo - Razzismo e xenofobia – art. 5, L. 20/11/2017, n. 167 – GU 27/11/2017	In vigore dal 12/12/2017
L.146/2006	Art. diversi	Reati transazionali art. 3 e 10 (Ratifica ed esecuzione protocollo Nazioni unite)	In vigore dal 12 aprile 2006

(1) Le parole: "nonché autoriciclaggio" sono state inserite nella rubrica dall'art. 3, c. 5, lett. b) della legge 15/12/2014, n. 186, con effetto dall'1/1/2015. Con la stessa norma (lett. b) è stato anche modificato il testo dell'art. 25-octies

(2) Il Dlgs n. 125/2016, in vigore dal 27/6/2016, ha modificato gli artt. 453 e 461 c.p. , richiamati dall'art. 25-bis del Dlgs. n. 231/2001

(3) La legge 9/1/2019, art. 1, comma 9, lett. b), n. 2 ha modificato l'art. 25, comma 1 introducendo l'art. 346 bis del codice penale rubricato "traffico di influenze illecite"

1.3 Le sanzioni

Il sistema sanzionatorio, descritto dal D. Lgs. 231/2001 a fronte del compimento dei reati sopra elencati, prevede, a seconda dei reati che sono commessi, l'applicazione delle seguenti sanzioni amministrative (art. 9):

a) sanzioni pecuniarie;

b) sanzioni interdittive;

c) confisca;

d) pubblicazione della sentenza.

Le sanzioni pecuniarie, che sono sempre applicate in caso di responsabilità dell'ente, sono determinate dal giudice attraverso un sistema basato su "quote".

L’importo della singola quota va da un minimo di euro 258,23 ad un massimo di euro 1.549,37 e viene fissato sulla base delle situazione economica/finanziaria dell’ente, allo scopo di assicurare l’effettività della sanzione. Il giudice determina il numero delle quote (in un numero non inferiore a 100 e non superiore a 1000) tenendo conto:

(1) della gravità del fatto;

(2) del grado della responsabilità dell’ente;

(3) dell’attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

Il valore della quota è fissato sulla base delle condizioni economico-patrimoniali dell’azienda allo scopo di assicurare l’efficacia della sanzione. Non è ammesso il pagamento in misura ridotta.

Le principali sanzioni interdittive, che nei reati di maggior rilievo si applicano in aggiunta alle sanzioni pecuniarie, sono rappresentate:

- dalla sospensione o revoca di autorizzazioni, licenze e concessioni;
- dal divieto di contrarre con la Pubblica Amministrazione;
- dall’interdizione dall’esercizio dell’attività;
- dall’esclusione o revoca di agevolazioni, finanziamenti e contributi;
- dal divieto di pubblicizzare beni e servizi.

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

- la società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;

- 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.

1.4 L'adozione di un "Modello di Organizzazione e di Gestione"

Oltre all'ipotesi in cui i soggetti apicali o subordinati abbiano agito nell'esclusivo interesse proprio o di terzi, l'art. 6 del Decreto n. 231, prevede una forma di esonero dalla responsabilità amministrativa qualora l'ente dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato un modello di organizzazione e di gestione idoneo a prevenire i reati considerati;

b) il compito di vigilare sul funzionamento e sull'osservanza del modello e di curare il suo aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo;

c) le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il modello di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza.

Lo stesso articolo prevede, inoltre, che, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di organizzazione e di gestione devono rispondere alle seguenti esigenze:

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

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

3) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;

4) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;

5) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;

6) prevedere, in relazione alla natura e alla dimensione dell'organizzazione nonché del tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

1.5 Finalità del Modello

Scopo del Modello è la costruzione di un sistema strutturato e organico di procedure organizzative di gestione e di attività di controllo volto a prevenire la commissione delle fattispecie di reato previste dalla norma tale da non poter essere aggirato se non intenzionalmente.

Il Modello rappresenta altresì un mezzo di divulgazione dei valori aziendali cui la società ha deciso di improntare la propria attività, oltre all'applicazione delle disposizioni di legge.

In particolare, attraverso l'individuazione delle aree di attività a rischio, il Modello si propone di:

- prevenire e ragionevolmente limitare i possibili rischi connessi all'attività aziendale con particolare riguardo ai rischi collegati alle condotte illegali;
- rendere consapevoli tutti coloro che operano nelle aree di attività a rischio di poter incorrere in un illecito passibile di sanzioni non solo nei propri confronti ma anche nei confronti dell'azienda escludendo che qualunque soggetto operante all'interno della Società possa giustificare la propria condotta adducendo l'ignoranza delle direttive aziendali;
- informare in ordine alle gravose conseguenze che potrebbero derivare alla società e indirettamente a tutti i portatori di interesse dall'applicazione delle sanzioni pecuniarie e interdittive previste dal Decreto e dalla possibilità che esse siano disposte anche in via cautelare;

- ribadire che la Società condanna i comportamenti contrari alle disposizioni di legge vigenti e che cerca in tutti i modi di evitare e prevenire tali comportamenti;
- consentire alla Società di intervenire tempestivamente per prevenire e contrastare la commissione dei reati stessi;
- eliminare eventuali carenze organizzative, soprattutto in materia di sicurezza, con l'obiettivo di scongiurare il verificarsi di infortuni sul lavoro, ponendo particolare attenzione, oltre all'aspetto prevenzionistico, anche a quello formativo, informativo e all'addestramento del personale in posizione c.d. "apicale".

1.6 Approvazione del modello e modifiche

Il presente Modello di organizzazione è soggetto all'approvazione degli Amministratori.

Le successive modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza degli Amministratori; è riconosciuta a ciascun Amministratore la facoltà di apportare al testo eventuali modifiche e integrazioni di carattere formale.

1.7 Sistema disciplinare

1.7.1 Principi generali

Aspetto essenziale per l'efficacia del Modello è costituito dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei reati di cui al Decreto e, in generale, delle procedure previste dal Modello stesso.

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

Allo stesso modo, la Unità di Compliance di Indra sarà informata e parteciperà con la Direzione aziendale alla valutazione degli opportuni provvedimenti da adottare in relazione alle irregolarità connesse alla perpetrazione delle infrazioni previste dal Decreto o a comportamenti non conformi al Modello, fermo restando che l'irrogazione delle sanzioni

sarà effettuata dalle funzioni aziendali preposte.

1.7.2 Sanzioni per i lavoratori dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente modello sono definiti come illeciti disciplinari in quanto ledono il rapporto di fiducia instaurato con l'azienda.

Con riferimento alle sanzioni irrogabili nei riguardi di detti lavoratori esse rientrano tra quelle previste dal C.C.N.L. Industria Metalmeccanica (art. 23 e seguenti) e sono applicabili nel rispetto delle procedure previste dall'art. 7 dello Statuto dei Lavoratori.

In particolare, in applicazione delle norme previste dal C.C.N.L., si prevede che:

1) incorre nei provvedimenti di RICHIAMO VERBALE o AMMONIZIONE SCRITTA

   il lavoratore che:

   - violi le procedure interne previste dal Modello o adotti, nell'espletamento diattività nelle aree a rischio, un comportamento non conforme alle prescrizioni dello stesso,

   dovendosi ravvisare in tali comportamenti una trasgressione delle disposizioni impartite e la mancata osservanza della disciplina aziendale;

2) incorre nel provvedimento della MULTA

   il lavoratore che:

   - violi più volte le procedure interne previste dal Modello o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conformealle prescrizioni dello stesso,

   dovendosi ravvisare in tali comportamenti una trasgressione di maggior rilievo delle disposizioni impartite e la ripetuta inosservanza della disciplina aziendale;

3) incorre nel provvedimento della SOSPENSIONE

   il lavoratore che:

   - nel violare le procedure interne previste dal Modello o adottando,nell'espletamento di attività nelle aree a rischio, un comportamento non conformealle prescrizioni

dello stesso, arrechi danno alla società o la esponga a una situazione oggettiva di pericolo per l'integrità dei beni dell'azienda,

dovendosi ravvisare in tali comportamenti la determinazione di un danno o di una situazione di pericolo per l'integrità dei beni dell'azienda derivanti dall'inosservanza delle disposizioni impartite e della disciplina aziendale;

4) incorre nel provvedimento del LICENZIAMENTO CON PREAVVISO

il lavoratore che:

- adotti nell'espletamento delle attività nelle aree a rischio un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto,

dovendosi ravvisare in tale comportamento la determinazione di un danno notevole o di una notevole situazione di pregiudizio per l'azienda derivanti da gravi infrazioni alla disciplina e alla diligenza del lavoro;

5) incorre nel provvedimento del LICENZIAMENTO SENZA PREAVVISO

il lavoratore che:

- adotti nell'espletamento delle attività nelle aree a rischio un comportamento palesemente in violazione alle prescrizioni del presente Modello e tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto,

dovendosi ravvisare in tale comportamento il compimento di atti tali da far venire meno il rapporto di fiducia nei confronti del dipendente ovvero che determinano un danno grave o un grave pregiudizio per l'azienda derivanti da una grave inosservanza delle disposizioni per l'esecuzione e per la disciplina del lavoro.

Il tipo e l'entità delle sanzioni sarà determinato in relazione:

- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- al comportamento complessivo del lavoratore con particolare riguardo alla

sussistenza o meno di precedenti disciplinari;

- al tipo di mansioni esplicate e all'entità della mancanza;
- alla posizione funzionale della persona coinvolta;
- alle circostanze del caso concreto.

1.7.3 Sanzioni per i dirigenti

In caso di violazione da parte dei dirigenti delle procedure previste dal 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 CCNL dei Dirigenti industriali.

1.7.4 Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte degli Amministratori, l'organo di vigilanza interno informerà tutti gli Amministratori e il Collegio Sindacale i quali provvederanno ad assumere le opportune iniziative previste dalla vigente normativa.

1.7.5 Misure nei confronti di Collaboratori esterni

Ogni comportamento posto in essere dai collaboratori esterni in contrasto con le linee di condotta indicate nel presente Modello e tale da comportare il rischio di commissione di un reato sanzionato dal Decreto potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla società.

2 Parte speciale A

2.1 Il codice etico

La società ha adottato un Codice Etico che è parte integrante del presente Modello.

2.2 Organo di vigilanza

2.2.1 Individuazione

Tenuto conto della dimensione e della semplicità della struttura organizzativa della Società nonché delle attività dalla stessa in concreto poste in essere nelle aree a rischio, il compito di vigilare sul funzionamento e sull'osservanza del Modello è affidato ad un Organo di vigilanza di natura monocratica.

È garantita, in ragione del posizionamento riconosciuto nel contesto dell'organigramma aziendale e delle linee di riporto attribuite, la necessaria autonomia dell'Organo di vigilanza.

Nello svolgimento delle attività di competenza e al fine di consentire la massima adesione ai requisiti e ai compiti di legge, l'Organismo di vigilanza nell'assolvimento dell'incarico attribuitogli:

- è supportato dal personale che svolge attività di internal audit nell'ambito del Sistema di Assicurazione della Qualità;
- si avvale delle specifiche professionalità dei consulenti esterni che collaborano con la Società per l'esecuzione delle operazioni tecniche, fermo restando l'obbligo del professionista di riferire all'organo interno;
- riferisce al Collegio Sindacale sull'eventuale commissione dei reati considerati o su eventuali carenze del Modello affinché questo si attivi secondo quanto previsto dalla legge.

2.2.2 Nomina

L'Organo di vigilanza è nominato dagli Amministratori che ne determinano il compenso annuo.

L’incarico è affidato a un professionista esperto in tematiche societarie, procedure dei controlli interni e dei rischi aziendali in grado di eseguire le funzioni e i compiti assegnati all’OdV, considerati i diversi settori in cui si svolge l’attività di verifica e controllo.

Egli non può ricoprire incarichi di gestione o esecutivi (per es. membro del Consiglio di Amministrazione), o di controllo (per es. del Collegio Sindacale), nella Società, o nelle altre società controllate o controllanti.

Costituiscono cause di ineleggibilità e di decadenza dell’Organismo di vigilanza e delle risorse umane dedicate:

1) la condanna con sentenza passata in giudicato per aver commesso uno dei reati previsti dal Decreto;
2) la condanna con sentenza passata in giudicato a pena che importa l’interdizione, anche temporanea, dai pubblici uffici, ovvero l’interdizione temporanea dagliuffici direttivi delle persone giuridiche e delle imprese;
3) la presenza di una delle circostanza descritte dall’art. 2382 c.c.;
4) l’esistenza di situazioni che compromettano seriamente l’autonomia e l’indipendenza dell’Organo di vigilanza.

In casi di particolare gravità, anche prima del giudicato, gli Amministratori potranno disporre la sospensione dei poteri dell’Organo di vigilanza e la nomina di un interim.

L’Organismo di vigilanza rimane in carica per tre anni; l’incarico può essere rinnovato da parte degli Amministratori. Nel caso di revoca, rinuncia, morte, del rappresentante dell’Organo, gli Amministratori provvedono con tempestività alla nuova nomina.

Fatta salva l’ipotesi di una rivisitazione del ruolo e del posizionamento dell’Organismo di vigilanza sulla base delle esperienze di attuazione del Modello, l’eventuale revoca degli specifici poteri allo stesso attribuiti potrà avvenire soltanto per giusta causa, previadelibera degli Amministratori.

2.2.3 Funzioni e poteri dell’Organo di vigilanza

All’Organo di vigilanza è affidato il compito di:

- vigilare sull'osservanza delle prescrizioni del Modello da parte dei destinatari appositamente individuati in relazione alle diverse tipologie di reati;
- verificare l'adeguatezza e la reale efficacia del Modello nel prevenire la commissione dei reati di cui al decreto con particolare attenzione all'identificazione delle aree "a rischio" reato, e alla idoneità delle procedure adottate alla prevenzione dei reati rilevanti;
- valutare il mantenimento nel tempo dei requisiti di funzionalità del Modello promuovendone il necessario aggiornamento in relazione alle mutate condizioni aziendali;
- promuovere e assicurare un'adeguata diffusione e conoscenza del Modello nei confronti dei dipendenti della Società e dei destinatari dello stesso;
- assicurare i flussi informativi di competenza.

A tal fine all'Organo di vigilanza sono altresì affidati i compiti di:

- elaborare le risultanze delle attività effettuate e la relativa reportistica;
- assicurare il mantenimento e l'aggiornamento del sistema di identificazione e classificazione delle aree a rischio ai fini dell'attività di vigilanza;
- promuovere e assicurare l'elaborazione di direttive per la struttura e i contenuti dei flussi informativi verso l'Organo di vigilanza;
- assicurare la gestione dei sistemi informativi sviluppati al fine dell'esercizio delle attività prescritte dal Modello;
- segnalare alle funzioni competenti la notizia di violazione del Modello e monitorare l'applicazione delle sanzioni disciplinari;
- promuovere e monitorare le iniziative per la diffusione della conoscenza del Modello, nonché per la formazione del personale e la sensibilizzazionedello stesso all'osservanza dei principi contenuti nel Modello.

Le attività poste in essere dall'Organismo di vigilanza non possono essere sindacate da alcun altro organismo o struttura aziendale. Gli Amministratori sono in ogni caso chiamati a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto,sugli stessi, grava in ultima istanza la responsabilità del funzionamento e dell'efficaciadel Modello organizzativo.

Nello svolgimento dei compiti assegnati, l'Organo di vigilanza ha accesso senza limitazioni alle informazioni aziendali per le attività d'indagine, analisi e controllo. È fatto obbligo di informazione in capo a qualunque funzione aziendale, dipendente o componente degli organi sociali, a fronte di richieste da parte dell'Organo di vigilanza o al verificarsi di eventi o circostanze rilevanti ai fini dello svolgimento delle attività di sua competenza.

L'Organo di vigilanza può avvalersi sotto la sua diretta sorveglianza e responsabilità dell'ausilio di tutte le strutture della Società e può chiedere o assegnare a consulenti esterni, in possesso delle competenze specifiche necessarie per la migliore esecuzione dell'incarico, compiti di natura meramente tecnica.

2.2.4 Reporting nei confronti degli organi societari

L'organo di vigilanza riferirà, su base continuativa, all'amministratore delegato e all'Unità di Compliance di Indra (che riferisce al Comitato di Audit e Conformità, comitato delegato del Consiglio di Amministrazione di Indra Sistemas, S.A.) in merito all'attuazione e al funzionamento del Modello o a situazioni specifiche di particolare rilievo.

Annualmente, inoltre, trasmetterà un rapporto scritto sull'attività svolta (i controlli e le verifiche specifiche effettuati e l'esito degli stessi, l'eventuale aggiornamento della mappatura dei processi sensibili, ecc.) agli Amministratori e al Collegio Sindacale così come alla Unità di Compliance di Indra.

2.2.5 Reporting verso l'Organo di vigilanza

All'Organo di vigilanza devono inoltre essere comunicate le seguenti informazioni:

- le notizie relative a cambiamenti organizzativi (es. organigrammi, procedure);

- gli aggiornamenti del sistema delle deleghe e dei poteri;
- le significative o atipiche operazioni interessate alle aree di rischio individuate;
- i mutamenti nelle situazioni di rischio o potenzialmente a rischio;
- le eventuali comunicazioni del Collegio Sindacale riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni.

2.2.6 Informazione e formazione del personale

Conformemente a quanto previsto dal Decreto, l'azienda ha definito un piano di comunicazione e formazione finalizzato a garantire una corretta divulgazione e conoscenza del Modello e delle regole di condotta in esso contenute nei confronti delle risorse già presenti in azienda e di quelle da inserire con differente grado di approfondimento in ragione del diverso livello di coinvolgimento nelle attività a rischio.

In relazione alla comunicazione del Modello, l'azienda si impegna a:

- diffondere il Modello attraverso la pubblicazione con gli strumenti ritenuti più idonei;

- predisporre uno specifico training destinato prioritariamente alle figure apicali.

In ogni caso, l'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. n. 231/2001 e le prescrizioni del Modello adottato saràdifferenziata nei contenuti e nelle modalità in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza dell'azienda.

3 Parte speciale B

3.1 Reati rilevanti

Ai sensi dell'art. 6 del Decreto, che prevede che la società individui le attività nel cui ambito possono essere commessi i reati, Smartest S.r.l. ha svolto un'analisi di tutte le attività aziendali, dei processi di formazione delle decisioni, nonché del sistema di controllo interno.

Sulla base dell'analisi sono stati individuati i soggetti, le attività e le categorie di operazioni per le quali esiste il rischio di commissione dei reati previsti dal Decreto.

I rischi individuati sono stati analizzati anche in funzione della probabilità di accadimento e dei controlli preventivi in essere; inoltre, ove ritenuto necessario, sono stati individuati gli eventuali opportuni adeguamenti al sistema di controllo.

Sulla base delle analisi di cui sopra e in considerazione della natura e dell'attività della Società, ai fini del Modello sono considerati rilevanti unicamente i seguenti reati :

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto)
- reati societari (art. 25-ter del Decreto)
- reati di omicidio colposo e lesioni colpose gravi e gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies del Decreto)
- reati di riciclaggio (art. 25-octies del Decreto)
- delitti informatici e trattamento illecito dei dati (art. 24-bis del Decreto)
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies del Decreto)

In relazione all'attività svolta dalla Smartest è stata valutata come remota la possibilità di commissione degli altri reati previsti dal Decreto.

3.2

3.3 Reati contro la Pubblica Amministrazione

3.3.1 La tipologia dei reati nei rapporti con la Pubblica Amministrazione

Le principali ipotesi di reato previste dagli articoli 24 e 25 del Decreto sono:

- ***Malversazione a danno dello Stato o dell'U.E. (art. 316-bis c.p.)***

Tale ipotesi di reato si configura nel caso in cui dopo avere ricevuto finanziamenti o contributi da parte dello Stato o dell'U.E., non si proceda all'utilizzo delle sommeottenute per gli scopi cui sono destinate.

Tenuto conto che il momento di attuazione del reato coincide con la fase esecutiva di impiego delle somme ricevute, lo stesso può insorgere anche con riferimento a finanziamenti già ottenuti in passato e che successivamente non siano destinati allefinalità per cui sono stati erogati.

- ***Indebita percezione di erogazioni in danno dello Stato e dell'U.E. (art. 316-ter c.p.)***

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo dallo Stato, da altri enti pubblici o dall'U.E..

In questo caso il reato, che si configura solo quando la condotta non integri gli estremi della truffa ai danni dello Stato, si realizza nel momento dell'ottenimento dei finanziamenti.

- ***Concussione (art. 317 c.p.)***

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli.

- ***Corruzione per un atto d'ufficio o 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 del corruttore.

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

Tale ipotesi di reato si configura nel caso in cui al fine di ottenere un vantaggio nell'ambito di un procedimento giudiziario in cui la società sia parte, si corrompa un pubblico ufficiale.

- ***Induzione indebita a dare o promettere utilità (art. 319-quater)***

Tale ipotesi di reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità. Commette il reato altresì il soggetto che dà o promette denaro o altra utilità.

- ***Traffico di influenze illecite (art. 346-bis)***

Commette questa ipotesi di reato "Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui 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 prezzodella 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".

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

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale rifiuti l'offerta illecitamente avanzatagli.

- ***Truffa in danno dello Stato, di altro Ente Pubblico o dell'U.E. (art. 640, comma 2 n. 1, c.p.)***

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato.

Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere al fine di ottenere l'aggiudicazione della gara stessa.

- ***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 ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

- ***Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.)***

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi.

3.3.2 Aree a rischio

La Società ha effettuato una dettagliata analisi dell'operatività aziendale ai fini dell'individuazione delle aree a rischio intendendosi per queste ultime le aree di attività che risultano interessate dalle potenziali casistiche di reato.

Poiché i reati considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione, le attività più specificamente a rischio sono individuate nelle aree di attività relative alla partecipazione a procedure competitive e al conseguimento di finanziamenti o contributi.

Tuttavia, l'analisi effettuata con specifico riferimento alle attività effettivamente svolte, ha evidenziato che allo stato attuale la realizzazione di fattispecie di reato connesse alla partecipazione a procedure di gara indette dalla Pubblica Amministrazione sia solo potenziale. Quanto previsto nel modello con riferimento a tali ipotesi di reato troverà applicazione al momento di effettivo svolgimento delle attività individuate.

Sono quindi considerate attività a rischio:

1) la partecipazione a procedure di gara o di negoziazione diretta indette da Enti Pubblici italiani o stranieri;
2) la partecipazione alle procedure di gara in associazione con partner;
3) l'assegnazione, ai fini della partecipazione alle procedure di gara, di specifici incarichi di consulenza o di rappresentanza a un soggetto terzo;
4) la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici;
5) l'assegnazione, ai fini della partecipazione alle procedure per l'ottenimento di erogazioni, contributi o finanziamenti, di specifici incarichi di consulenza a un soggetto terzo;
6) il concreto impiego di erogazioni, contributi o finanziamenti ottenuti da parte di organismi pubblici e più in generale le modalità di impiego delle risorse finanziarie.

3.3.3 Principi di comportamento e di attuazione del processo decisionale nelle aree a rischio

Con riferimento agli ambiti di attività individuati è vietato ai dipendenti e ai responsabili aziendali nonché ai collaboratori esterni e ai partner attraverso apposite clausole contrattuali 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, possano potenzialmente diventarlo;
3) porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione alle suddette ipotesi di reato.

Nell'ambito di tali comportamenti è fatto in particolare divieto di:

a) effettuare elargizioni in denaro a pubblici funzionari;

b) distribuire omaggi e regali eccedenti le normali pratiche commerciali o di cortesia o che siano comunque rivolti ad acquisire trattamenti di favore nella conduzione di qualsiasi attività. In particolare è vietata qualsiasi forma di regalo a funzionari pubblici, 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;

c) accordare altri vantaggi di qualsiasi natura (promesse di assunzioni, di affidamento di incarichi, ecc.) in favore di funzionari pubblici, o loro familiari,che possano influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;

d) effettuare prestazioni in favore di partner che non trovino adeguata giustificazione nel contesto del rapporto associativo;

e) riconoscere compensi in favore di collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;

f) riconoscere compensi o effettuare prestazioni in favore di chiunque offra la propria mediazione sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di pubblico servizio;

g) presentare dichiarazioni non veritiere a organismi pubblici al fine di ottenere erogazioni pubbliche, contributi o finanziamenti agevolati;

h) destinare somme ricevute da organismi pubblici a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- i rapporti nei confronti della Pubblica Amministrazione per le suddette aree di attività a rischio devono essere gestiti, a seconda dei casi, dal responsabile commerciale o dal responsabile amministrativo;

- gli incarichi conferiti ai collaboratori esterni e gli accordi di associazione con i partner per attività rientranti nelle aree a rischio devono essere definiti per iscritto, verificati dal responsabile amministrativo e approvati da un amministratore. Devono, inoltre, essere inserite nei contratti specifiche clausole dirette a vietare comportamenti tali da integrare fattispecie di reato considerate nel decreto;
- non possono essere effettuati pagamenti in contanti a fornitori per importi pari o superiori a 1.000,00 euro;
- le dichiarazioni rese a organismi pubblici ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamenteveritieri, e devono essere verificati dal responsabile amministrativo e approvate da un amministratore;
- in caso di ottenimento da parte di organismi pubblici di erogazioni, contributi o finanziamenti l'effettivo sostenimento delle spese agevolate deve essere verificato dal responsabile amministrativo e da un amministratore;
- tutte le irregolarità e le violazioni alle prescrizioni del presente Modello da chiunque rilevate devono essere tempestivamente comunicate all'organo di vigilanza interno.

Premesso che le modalità di attuazione degli acquisti e delle offerte ai clienti sono già disciplinate dalle procedure del Sistema di Gestione per la Qualità, che già prevedono delle specifiche attività di controllo, si ritiene sufficiente adottare le seguenti modalità di gestione.

Per ogni singola operazione a rischio un amministratore nominerà un responsabile che provvederà a compilare un'apposita scheda da tenere aggiornata nel corso dello svolgimento della procedura da cui risulti:

- la descrizione dell'operazione a rischio e del suo valore economico;
- la Pubblica Amministrazione che ha competenza sulla procedura;
- il nome del responsabile interno e la sua posizione nell'ambito dell'organizzazione aziendale;

- la dichiarazione del responsabile di essere a conoscenza degli adempimenti da espletare e degli obblighi da osservare nello svolgimento dell'operazione e che non è incorso in reati considerati dal Decreto;
- l'indicazione dei principali adempimenti svolti nell'espletamento dell'operazione;
- il nome del funzionario della Pubblica Amministrazione con cui vengono intrattenuti rapporti e la sua posizione nell'ambito dell'organizzazione;
- il nome del funzionario della Pubblica Amministrazione responsabile del procedimento;
- l'indicazione di eventuali collaboratori esterni, dell'incarico conferito e del corrispettivo pattuito;
- altre circostanze e notizie ritenute utili (es. pagamenti effettuati nell'ambito dell'operazione).

Il responsabile dovrà tenere la scheda a disposizione dell'organo di vigilanza interno e inviarne allo stesso una copia all'avvio e alla chiusura dell'operazione.

3.4 Reati societari

3.4.1 Le tipologie dei reati societari

Il D.lgs. 11 aprile 2002 n. 61, nel dettare la nuova disciplina dei reati societari, ha previsto la responsabilità amministrativa della società in relazione ai reati in materia societaria, se commessi nell'interesse della società da amministratori, direttori generali o liquidatori o persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se avessero vigilato in conformità degli obblighi inerenti alla loro carica.

I principali reati societari previsti dall'art. 25-ter del Decreto sono:

- ***False comunicazioni sociali (art. 2621 e 2622 c.c.)***

Il reato si realizza quando gli amministratori, i direttori generali, i sindaci e i liquidatori, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per gli altri un ingiusto profitto, espongono nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, fatti materiali non rispondenti al vero ancorché oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale e finanziaria della società o del gruppo alla quale essa appartiene, in modo idoneo a indurre in errore i destinataridelle indicate comunicazioni sociali.

Ai fini della punibilità è necessario (i) che le informazioni false o omesse siano tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società e (ii) che intervenga una querela di parte, salvo che il reato sia commesso in danno dello Stato, di altri Enti Pubblici, dell'Unione Europea o che si tratti di società quotate nel qual caso è prevista la procedibilità d'ufficio.

- ***Falso in prospetto (art. 2623 c.c.)***

Tale ipotesi di reato consiste (i) nell'esporre false informazioni ovvero nell'occultare dati o notizie nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio con la consapevolezza della falsità e l'intenzione di ingannare (ii) in modo idoneo a indurre in

errore i destinatari dei prospetti stessi e (iii) allo scopo di conseguire per sé o per altri un ingiusto profitto.

- ***Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 c.c.)***

Incorrono in tale tipo di reato i responsabili della revisione che, al fine di conseguire per sé o per altri un ingiusto profitto, attestano il falso ovvero occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società nelle relazioni o in altre comunicazioni in modo idoneo a indurre i destinatari delle stesse in errore. Affinché si realizzi l'ipotesi di reato deve sussistere la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni.

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

Tale ipotesi di reato si realizza quando gli amministratori, al di fuori dei casi di legittima riduzione del capitale sociale, restituiscono anche simulatamene i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

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

Incorrono in questo reato gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite.

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

Commettono tale reato gli amministratori che, fuori dai casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

- ***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 fusioni con altre società o scissioni che cagionano danno ai creditori.

Soggetti attivi del reato sono gli amministratori che sono puniti a querela della persona offesa.

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

Incorrono in tale reato gli amministratori o i soci che formano o aumentano fittiziamente il capitale sociale mediante: a) attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale; b) sottoscrizione reciproca di azioni o quote; c) sopravvalutazione rilevante dei conferimenti di beni in natura o di creditiovvero del patrimonio della società nel caso di trasformazione.

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

Tale ipotesi di reato consiste nella ripartizione, effettuata dai liquidatori, di beni sociali tra i soci, prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni danno ai creditori.

- ***Impedito controllo (art. 2625 c.c.)***

Commettono tale reato gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione.

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

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con attisimulati o fraudolenti allo scopo di procurare a sé o ad altri un ingiusto profitto.

- ***Aggiotaggio (art. 2637 c.c.)***

Tale ipotesi di reato consiste nella diffusione di notizie false ovvero nella realizzazione di operazioni simulate o di altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, quotati o non quotati, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

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

Il reato si realizza quando gli amministratori, i direttori generali, i sindaci e i liquidatori, nelle comunicazioni previste per legge alle Autorità pubbliche di Vigilanza espongono, al fine di ostacolare l'esercizio delle funzioni di vigilanza, fatti non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria ovvero occultano con altri mezzi fraudolenti, in tutto o in parte, fatti che avrebberodovuto comunicare concernenti la situazione medesima.

Il reato si realizza anche con il semplice ostacolo all'esercizio delle funzioni di vigilanza attuato intenzionalmente e in qualsiasi forma anche omettendo le comunicazioni dovute.

3.4.2 Aree a rischio

Essendo costituita nella forma della società a responsabilità limitata, la Società è esposta al rischio di commissione di alcuni reati societari o comunque connessiall'amministrazione e gestione di un'azienda che opera con criteri privatistici. Poiché la Società non opera sul mercato degli strumenti finanziari, allo stato attuale, all'interno dell'azienda possono essere realizzate solo alcune delle fattispecie di reato previste.

In relazione ai reati considerati, ai fini del presente Modello, sono ritenute più specificamente a rischio le aree di attività relative alla:

1) predisposizione di comunicazioni dirette ai soci e al pubblico in genere riguardo alla situazione economica, patrimoniale e finanziaria della società (bilancio d'esercizio);
2) predisposizione di prospetti informativi;
3) gestione dei rapporti con gli organi di controllo (collegio sindacale, organo incaricato del controllo contabile, ecc.).

Eventuali integrazioni delle aree di attività a rischio sono disposte dagli Amministratori ai quali viene dato mandato di analizzare il sistema di controllo previsto e di definire gli opportuni provvedimenti operativi.

3.4.3 Principi di comportamento

Tutti i soggetti coinvolti nello svolgimento delle attività nelle aree a rischio debbono attenersi a regole di condotta conformi a quanto prescritto nel presente Modello al fine di prevenire e impedire il verificarsi dei reati societari.

In particolare, nell'espletamento delle attività considerate a rischio dovranno essere osservati i seguenti principi generali di condotta:

1) astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati Societari;

2) astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

3) tenere un comportamento corretto e trasparente, assicurando il pieno rispetto delle norme di legge e regolamentari nello svolgimento delle attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci e al pubblico in generale una informazione veritiera e appropriata.

   È pertanto fatto divieto di:

   - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della situazione economica, patrimoniale e finanziaria della società;
   - omettere di comunicare dati e informazioni richiesti dalla normativa riguardo alla situazione economica, patrimoniale e finanziaria della società.

4) osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale al fine di non ledere le garanzie dei creditori edei terzi al riguardo.

5) assicurare il regolare funzionamento degli organi sociali garantendo e agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare.

È pertanto fatto divieto di:

- tenere comportamenti che impediscono materialmente o che comunque ostacolano, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o dell'organo incaricato del controllo contabile;
- porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

3.4.4 Procedure specifiche

In relazione allo svolgimento delle attività delle aree a rischio, devono essere rispettate le seguenti procedure:

1. nelle attività di predisposizione delle comunicazioni indirizzate ai soci e al pubblico in generale e, in particolare, ai fini della formazione del bilancio dovrà essere seguito il seguente procedimento:

a) il responsabile della funzione Amministrazione è tenuto a rilasciare un'apposita dichiarazione, convalidata da un amministratore, attestante:

- la veridicità, correttezza, precisione e completezza dei dati e delle informazioni contenute nel bilancio ovvero negli altri documenti contabili e nei documenti connessi;
- la predisposizione di un adeguato sistema di controllo interno teso a fornire una ragionevole certezza sui dati di bilancio;
- il rispetto delle procedure previste dal presente Modello.

b) la dichiarazione deve essere:

- presentata agli Amministratori in occasione dell'approvazione del progetto di bilancio civilistico;
- trasmessa in copia all'organo di vigilanza interno.

2. nelle attività di predisposizione dei prospetti informativi dovranno essere osservate le seguenti procedure:
   - quando non sia possibile verificare l'attendibilità dei dati acquisire un'attestazione di veridicità da parte dei soggetti da cui l'informazione proviene;
   - accertamento dell'idoneità sul piano professionale dei soggetti preposti alla predisposizione dei documenti
3. nella gestione dei rapporti con i componenti del Collegio Sindacale e dell'organo incaricato del controllo contabile dovranno essere osservate le seguenti disposizioni:
   - divieto di attribuire ai componenti del Collegio Sindacale o dell'organo a cui è demandato il controllo contabile incarichi di consulenza di qualsiasi natura;
   - divieto di stipula di contratti di consulenza con professionisti associati ai componenti del Collegio Sindacale e dell'organo a cui è demandato il controllo contabile;
   - divieto di stipula di contratti di consulenza, di collaborazione o di lavoro dipendente con i familiari (coniuge non separato, parente/affine in linea retta di 2° grado) dei componenti del Collegio Sindacale o dell'organo a cui è demandato il controllo contabile.

3.4.5 Verifiche dell'organo di vigilanza

I compiti di vigilanza dell'organo di vigilanza interno in relazione all'osservanza del modello per la parte relativa ai reati societari sono i seguenti:

1) con riferimento al bilancio, alle relazioni e alle comunicazioni sociali, l'organo di vigilanza:
    - verifica l'applicazione delle prescrizioni e l'efficacia delle procedure interne a prevenire il reato di false comunicazioni sociali;
    - esamina le eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente;
    - vigila sull'effettiva sussistenza delle condizioni per garantire l'autonomia e l'indipendenza del Collegio Sindacale e dell'organo incaricato del controllo contabile.
2) con riferimento alle altre attività a rischio:
    - verifica il rispetto delle procedure e l'efficacia delle stesse a prevenire la commissione dei reati;
    - esamina le eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente.

3.5 Reati di riciclaggio

3.5.1 Le tipologie dei reati di riciclaggio

I reati di riciclaggio sono stati introdotti nel corpus del D.Lgs. 231del 2001, all'art. 25-octies, dal D. Lgs. 231 del 21 novembre 2007 (di seguito "Decreto Antiriciclaggio") e assumono rilevanza anche se le attività che hanno generato i beni da riciclare si sono svolte nel territorio di un altro Stato comunitario o di un Paese extracomunitario.

Le principali ipotesi di reato sono qui di seguito elencate:

- ***Ricettazione (art. 648 cod. pen.)***

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta danaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farli acquistare, ricevere od occultare.

- ***Riciclaggio (art. 648-bis cod. pen.)***

Tale ipotesi di reato si configura nel caso in cui un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

- ***Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter cod. pen.)***

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto.

La normativa italiana in tema di prevenzione dei Reati di Riciclaggio prevede norme tese ad ostacolare le pratiche di riciclaggio, vietando tra l'altro l’effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l’identificazione della clientela e la registrazione dei dati in appositi archivi.

Il Decreto Antiriciclaggio prevede in sostanza i seguenti strumenti di contrasto del fenomeno del riciclaggio di proventi illeciti:

1. la previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiore a euro 1.000 (limite così modificato dal D.L. 201/2011);

2. l'obbligo di adeguata verifica della clientela da parte di alcuni soggetti destinatari del Decreto Antiriciclaggio in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi;

3. l'obbligo da parte di alcuni soggetti di conservare, nei limiti previsti dall'art. 36 del Decreto Antiriciclaggio, i documenti o le copie degli stessi e registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;

4. l'obbligo di segnalazione da parte di alcuni soggetti all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo.

I soggetti sottoposti agli obblighi di cui ai punti n. 2, 3 e 4 sono:

1) gli intermediari finanziari e gli altri soggetti esercenti attività finanziaria. Tra tali soggetti figurano, ad esempio: banche; poste italiane; società di intermediazione mobiliare (SIM); società di gestione del risparmio (SGR); società di investimento acapitale variabile (SICAV).

2) I professionisti, tra i quali si indicano:

• i soggetti iscritti nell'albo dei dottori commercialisti, dei ragionieri e periti commerciali;

• i notai e gli avvocati quando, in nome e per conto dei loro clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i loro clienti in determinate operazioni.

3) I revisori contabili.

4) Altri soggetti, intesi quali operatori che svolgono alcune attività il cui esercizio resta subordinato al possesso delle licenze, autorizzazioni, iscrizioni in albi o registri, ovvero alla preventiva dichiarazione di inizio di attività richieste dalle norme. Tra le attività si indicano:

• recupero di crediti per conto terzi;

• trasporto di denaro contante;

• gestione di case da gioco;

• offerta, attraverso internet, di giochi, scommesse o concorsi pronostici con vincite in denaro.

Come emerge dall'elencazione appena riportata, Smartest non figura tra i destinatari del Decreto Antiriciclaggio; tuttavia, gli Esponenti Aziendali possono astrattamente commettere uno dei Reati di Riciclaggio.

L'art. 25-octies del Decreto 231 ("Ricettazione, riciclaggio e impiego di denaro, beni o utilita' di provenienza illecita"), può pertanto applicarsi a Smartest.

3.5.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere le seguenti:

1. rapporti con fornitori e partner;

2. relazioni con controparti, diverse da partner e fornitori;

3. flussi finanziari in entrata;

4. rapporti infragruppo.

3.5.3 Principi di comportamento

Obiettivo delle prescrizioni è che gli Esponenti Aziendali, nella misura in cui possano essere coinvolti nello svolgimento di attività nelle Aree a Rischio, si attengano a regole di

condotta conformi a quanto prescritto al fine di prevenire ed impedire il verificarsi dei Reati di Riciclaggio.

In particolare, nell'espletamento delle attività considerate a rischio, gli Esponenti Aziendali, tramite apposite clausole contrattuali, in relazione al tipo di rapporto in essere con la società, dovranno attenersi ai seguenti principi generali di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati di Riciclaggio;

2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

3. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;

4. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;

5. effettuare un costante monitoraggio dei flussi finanziari aziendali.

3.5.4 Procedure specifiche

In relazione allo svolgimento delle attività delle aree a rischio, devono essere rispettate le seguenti procedure aziendali:

a) verificare l'attendibilità commerciale e professionale dei fornitori e partner commerciali e finanziari;

b) garantire trasparenza e tracciabilità degli accordi/joint venture con altre imprese per la realizzazione di investimenti;

c) procedere all'identificazione e registrazione dei dati delle persone fisiche e giuridiche con cui la Società conclude contratti di acquisto e verificare che tali soggetti non abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non

cooperativi dal Gruppo di Azione Finanziaria contro il riciclaggio di denaro (GAFI); qualora le controparti di cui alla presente area di rischio siano in alcun modo collegate ad uno di tali Paesi, sarà necessario che le decisioni relative ottengano l'espressa autorizzazione di un Amministratore, sentito l'Odv.

d) effettuare controlli formali e sostanziali dei flussi finanziari aziendali in entrata; tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo ecc.), degli Istituti di credito utilizzati (sede dellebanche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;

e) non accettare denaro e titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) per importi complessivamente pari o superiori a euro 1.000, se non tramite intermediari a ciò abilitati, quali banche, istituti di moneta elettronica e Poste Italiane S.p.A..

3.6 Reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

3.6.1 Le tipologie di reato

In questa sezione sono individuate le aree di attività nel cui ambito possono essere commessi i reati di omicidio colposo e lesioni colpose gravi e gravissime, di cui all'art. 25 septies del D. Lgs. 231/2001.

- ***Omicidio Colposo (art. 589 c.p.)***

Tale ipotesi di reato si configura nel caso in cui la Società nello svolgimento delle proprie attività, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni per colpa la morte di una persona.

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

Tale ipotesi di reato si configura nel caso in cui la Società nello svolgimento delle proprie attività, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni per colpa lesioni personali gravi o gravissime.

La lesione personale è grave:

1) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;

2) se il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione personale è gravissima se dal fatto deriva:

1) una malattia certamente o probabilmente insanabile;

2) la perdita di un senso;

3) la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;

4) la deformazione, ovvero lo sfregio permanente del viso.

3.6.2 Aree a rischio

In considerazione delle attività svolte dalla Smartest e della struttura interna adottata, ai sensi dell'art. 6 del Decreto, nonché sulla base del documento di valutazione dei rischi, predisposto ai sensi del D. Lgs. 9 aprile 2008 n. 81 e sue successive modifiche ed integrazioni, sono individuate le seguenti categorie di operazioni e attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25 septies del Decreto:

a) attività di ricezione di documentazione da digitalizzare, di scarico e movimentazione della stessa;

b) attività di manutenzione di impianti e macchinari tramite l'impiego di personale interno o esterno alla Società;

c) attività di manutenzione dei fabbricati e degli impianti della Società o in uso alla stessa inclusi i locali adibiti ad ufficio;

d) attività di manutenzione e movimentazione di mobili, arredi e delle attrezzature in uso alla Società;

e) attività lavorative con utilizzo di videoterminali;

f) accesso, transito e permanenza nei locali in uso alla Società, nello svolgimento delle sue attività da parte di Dipendenti e soggetti esterni, tra i quali sono inclusi anche iclienti.

3.6.3 Principi di comportamento

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del D. Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendalipreviste nella presente sezione.

Al fine di evitare il verificarsi dei reati di omicidio colposo e lesioni colpose gravi e gravissime, tutti i Destinatari del presente Modello devono attenersi alle specifiche regole e procedure che sono e saranno predisposte e diffuse dal Servizio Prevenzione e

Protezione della Società, istituito ai sensi del D. Lgs. 9 aprile 2008 n. 81 e sue successive modifiche ed integrazioni.

Fermo restando quanto sopra i Destinatari del presente Modello devono attenersi alle seguenti condotte:

a) osservare rigorosamente tutte le leggi e i regolamenti e procedure in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro che disciplinano l'accesso, il transito e lo svolgimento delle attività lavorative presso i locali in uso alla Società;

b) partecipare ai corsi organizzati dalla Società in materia di sicurezza sul lavoro, sulla tutela dell'igiene e salute sul lavoro e sullo svolgimento delle specifiche mansioni, ai quali saranno invitati;

c) fornire adeguati dispositivi di protezione individuali conformi alle normative vigenti e in funzione delle mansioni svolte;

d) identificare e delimitare il perimetro delle aree di lavoro interessate alle attività a rischio di manutenzione e nuova realizzazione in modo da impedire l'accesso a tali aree asoggetti non autorizzati ai lavori;

e) seguire, nella redazione, sottoscrizione ed esecuzione dei contratti, le regole di sicurezza che sono e saranno diffuse dal Servizio Prevenzione e Protezione della Società;

f) richiedere ai fornitori e agli altri destinatari esterni alla Società, ove richiesto da norme e regolamenti, in base alla natura del bene e servizio prestato, l'evidenza del rispetto delle normative sulla sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro;

g) segnalare alle funzioni competenti eventuali inefficienze dei dispositivi di protezione individuali ovvero di altri presidi a tutela della sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro.

È, inoltre vietato:

a) utilizzare, nello svolgimento delle attività identificate a rischio macchinari, attrezzature, strumenti utensili, materiali e dispositivi di protezione individuali non adeguati e non conformi alle normative vigenti per le specifiche operazioni da svolgere;

b) disattivare o rendere anche parzialmente inefficienti dispositivi individuali o collettivi di protezione;

c) nell'ambito degli interventi e attività di cui si è incaricati, svolgere attività ed operazioni al di fuori delle aree specificatamente identificate per gli interventi richiesti;

d) accedere ad aree di lavoro alle quali non si è autorizzati;

e) per i fornitori, utilizzare macchinari e attrezzature, strumenti utensili, materiali e dispositivi di protezione individuali di proprietà dalla Società.

3.6.4 Procedure specifiche

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, e nell'ambito specifico della gestione della sicurezza sul lavoro e della tutela dell'igiene e salute sul lavoro, nel rispetto di quanto previsto ai sensi del D. Lgs. 9 aprile 2008 n. 81 e sue successive modifiche ed integrazioni, sono previste specifiche procedure, in forza delle quali:

a) sono periodicamente individuati dal Servizio Prevenzione e Protezione i rischi in materia di sicurezza e tutela dell'igiene e salute sul lavoro, tenendo in adeguata considerazione: la struttura aziendale, la natura delle attività, l'ubicazione dei locali e delle aree di lavoro, l'organizzazione del personale, le specifiche sostanze, macchinari, attrezzature e impianti impiegati nelle attività e i relativi cicli di produzione;

b) è aggiornato, periodicamente ed in occasione di significative modifiche organizzative, il documento di valutazione dei rischi, redatto ai sensi del D. Lgs. 9 aprile 2008 n. 81 e sue successive modifiche ed integrazioni;

c) il Servizio Prevenzione e Protezione nella valutazione dei rischi adotti criteri oggettivi, documentati e ripetibili, considerando, per ogni specifico rischio come sopra individuato, la probabilità di accadimento, la dimensione dell'impatto del danno possibile, i risultati di

rilievi ambientali e la storia degli infortuni verificatisi nello svolgimento della specifica attività;

d) vengono definiti e periodicamente aggiornati il piano di intervento delle azioni di prevenzione e protezione sulla base del risultato della valutazione dei rischi effettuata, nonché i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute;

e) il Servizio Prevenzione e Protezione proponga e diffonda adeguate procedure volte alla tutela della sicurezza sul lavoro e alla tutela dell'igiene e salute sul lavoro nonché le indicazioni sulle adeguate misure di prevenzione e protezione da adottare, tenendo in adeguata considerazione quanto descritto nei punti precedenti e la normativa vigente in materia di sicurezza e tutela dell'igiene e salute sul lavoro;

f) i dirigenti e i preposti siano tenuti a sorvegliare sull'effettivo rispetto delle procedure proposte e diffuse dal Servizio Prevenzione e Protezione e sulla adozione delle adeguate misure di prevenzione e protezione, comunicando tempestivamente al Servizio Prevenzione e Protezione eventuali eccezioni e criticità;

g) venga definito il metodo di individuazione, segnalazione e comportamento da tenere in caso di emergenze, sia per gli addetti alla gestione delle specifiche emergenze che per gli altri soggetti che possono esserne coinvolti;

h) i lavoratori in base agli specifici rischi individuati a cui sono soggetti ricevano adeguata informazione e formazione in merito alla misure di prevenzione e protezione da adottare nello svolgimento delle proprie attività e gestione delle emergenze, in base alla normativa vigente in materia di sicurezza e tutela dell'igiene e salute sul lavoro e delle procedure proposte e diffuse dal Servizio Prevenzione e Protezione;

i) non siano corrisposti compensi a Fornitori in misura non congrua rispetto alle prestazioni rese alla Società o comunque non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;

l) alle ispezioni giudiziarie e amministrative (es. relative al D. Lgs. 9 aprile 2008 n. 81, ecc.) partecipino i soggetti a ciò espressamente delegati. L'OdV dovrà essereprontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della Funzione aziendale di volta in volta interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti appositi verbali, che verranno conservati dall'OdV;

m) siano previsti obblighi di riporto periodico all'OdV per le valutazioni di competenza con riguardo a quanto previsto dal presente modello.

3.7 Delitti informatici e trattamento illecito di dati

3.7.1 Le tipologie di reato

La legge 18 marzo 2008, n. 48, ratificando la Convenzione di Budapest del 23 novembre 2001, ha introdotto nel codice penale nuove fattispecie di reato relative ai delitti informatici ed al trattamento illecito dei dati e ha aggiunto all'art. 24-bis del Decreto l'elenco dei reati che possono comportare la responsabilità amministrativa degli enti.

Le principali ipotesi di reato previste dalla legge sono:

- ***Documenti informatici (art. 491-bis cod. pen.)***

L'articolo in oggetto stabilisce che la disciplina penale prevista per i delitti relativi alla falsità in atti (cfr. Codice Penale Capo III, Titolo VII, Libro II), tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, si applichi anche nel caso in cui la condotta riguardi non un documento cartaceo ma un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali. A titolo esemplificativo, integra il delitto di falsità in documenti informatici la condotta di chi utilizzi la firma elettronica altrui, falsifichi documenti aziendali oggetto di flussi informatizzati con una Pubblica Amministrazione o distrugga o occulti documenti veri.

- ***Accesso abusivo a un sistema informatico o telematico (art. 615-ter cod. pen.)***

Tale reato si realizza quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi permane contro la volontà del titolare del sistema. A tal riguardo si evidenzia come il legislatore abbia inteso punire l'accesso abusivo ad un sistema informatico o telematico anche quando lo stesso non sia seguito da un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto accede abusivamente ad un sistema informatico e, pur non effettuando alcuna sottrazione materiale di file, procede alla stampa o alla copia di un documento contenuto nell'archivio del personal computer altrui o anche alla sola visualizzazione delle informazioni in esso contenute. La suddetta fattispecie delittuosa si realizza altresì

nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si trattenga contro la volontà del titolare o utilizzi il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato. Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un dipendente, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza essere legittimato, a banche dati della società o di clienti per prendere cognizione didati riservati mediante l'utilizzo delle credenziali di altri soggetti. Il reato può configurarsi altresì quando un dipendente accede abusivamente al sistema informatico di un concorrente al fine di conoscere l'offerta economica presentata per la partecipazione a una gara di appalto o di acquisire informazioni sul portafoglio clienti.

- ***Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. pen.)***

L'art. 615 quater punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei a consentire l'accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo. La norma, al fine di prevenire le ipotesi di accesso abusivo a sistemi informatici, punisce anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi o di dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici. Potrebbe rispondere del delitto, ad esempio, il dipendente della società che comunichi a un altro soggetto la password di accesso al personal computer o alle caselle e-mail di un proprio collega allo scopo di consentire il controllo delle attività da questi svolte, quando ciò possa avere un determinato interesse per la società.

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

Tale reato si realizza qualora qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi a esso pertinenti,

ovvero di favorire l'interruzione o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici. Tale delitto potrebbe ad esempio configurarsi qualora un dipendente si procuri un Virus idoneo a danneggiare o a interrompere il funzionamento del sistema informatico delle aziende concorrenti.

- ***Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. pen.)***

Tale ipotesi di reato consiste nell'intercettare fraudolentemente comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento o interruzione di tali comunicazioni, nonché nella diffusione, parziale o integrale, del contenuto delle predette comunicazioni al pubblico mediante qualsiasi mezzo di informazione. Mediante dispositivi tecnici o l'uso di software di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione. Il reato potrebbe configurarsi, ad esempio, con il vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati o l'offerta per la partecipazione a una gara.

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

Questa fattispecie di reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi. La condotta vietata dall'art. 617-quinquies cod. pen. è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva. Il reato si integra, ad

esempio, a vantaggio della società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.

- ***Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. pen.)***

L'art. 635-bis c.p. punisce chiunque distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui. Il danneggiamento potrebbe essere commesso a vantaggio della società laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano effettuate al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui siano danneggiati dei dati aziendali "compromettenti".

- ***Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter cod. pen.)***

Tale reato si realizza quando un soggetto commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o a essi pertinenti, o comunque di pubblica utilità. Tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento riguarda beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di naturapubblica. Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici, aventi efficacia probatoria, registrati presso enti pubblici (es. polizia giudiziaria) relativi ad un procedimento penale a carico della società.

- ***Danneggiamento di sistemi informatici o telematici (art. 635-quater cod. pen.)***

Questo reato si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis cod. pen., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni oprogrammi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informaticio telematici altrui o ne ostacoli gravemente il funzionamento. Pertanto qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis cod.pen.

- ***Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cod. pen.)***

Questo reato si configura quando la condotta di cui al precedente art. 635-quater cod. pen. sia diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art. 635-ter cod. pen., quel che rileva è in primo luogo che il danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

- ***Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art.640-quinquies c.p.)***

Questo reato si configura quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, o di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Il soggetto attivo del reato può quindi essere soltanto un certificatore qualificato che esercita particolari funzioni di certificazione per la firma elettronica qualificata. A tale proposito si osserva che la società non riveste la qualifica di "certificatore qualificato" e che pertanto non può incorrere nell'ipotesi di reato.

*****

Si precisa in ogni caso che la commissione di uno dei Delitti Informatici sopra descritti assume rilevanza, per le finalità di cui al Decreto, solo qualora la condotta, indipendentemente dalla natura aziendale o meno dei dati, informazioni, programmi, sistema informatico o telematico, possa determinare un interesse o vantaggio per lasocietà. Pertanto, nell'ambito della descrizione delle singole fattispecie criminose, si è tenuto conto di tale aspetto per l'elaborazione dei casi pratici proposti.

3.7.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere le seguenti:

1. tutte le attività aziendali svolte tramite l'utilizzo dei sistemi informatici aziendali e dei clienti, del servizio di posta elettronica e dell'accesso ad Internet;

2. gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione;

3. gestione dei flussi informativi elettronici con la pubblica amministrazione.

3.7.3 Principi di comportamento

Obiettivo della presente sezione è che i Destinatari si attengano, nella misura in cui siano coinvolti nello svolgimento delle attività rientranti nelle Aree a Rischio, a regole di condotta idonee a prevenire e impedire il verificarsi dei Delitti Informatici.

In particolare, la presente sezione ha la funzione di:

a) fornire un elenco dei principi generali e dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;

b) fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.

L'utilizzo e la gestione di sistemi informatici sono imprescindibili per lo svolgimento dell'attività aziendale e contraddistinguono la maggior parte dei processi produttivi. Tra i sistemi informativi utilizzati dalla Smartest S.r.l. vi sono altresì hardware e software per

l'espletamento di attività che prevedono il ricorso a specifici programmi forniti dai clienti ovvero la connessione diretta con i sistemi informativi degli stessi. Si rende quindi necessaria un'efficace definizione di norme e misure di sicurezza organizzative e comportamentali e la realizzazione di attività di controllo atte a garantire una gestione e un utilizzo dei sistemi informatici coerente con la normativa vigente.

Nell'espletamento delle rispettive attività tutte le figure professionali coinvolte nei processi aziendali, oltre alle regole di cui al presente Modello, sono tenuti, in generale, a rispettare tutte le regole e i principi contenuti nelle procedure e istruzioni operative adottate da Smartest in tema di Sicurezza Informatica che riguardano, a titolo esemplificativo: uso delle risorse informatiche, controllo degli accessi logici alle risorse informatiche, gestione degli incidenti di sicurezza delle informazioni e reazione ai medesimi, sicurezza della rete e delle comunicazioni.

Smartest S.r.l. ha attribuito la massima rilevanza alla individuazione e adozione di misure adeguate di sicurezza – di natura organizzativa, fisica e logica – in modo da minimizzare il rischio di accessi non autorizzati, di alterazione, di divulgazione, di perdita o di distruzione delle risorse informatiche.

Accanto al rispetto dei principi procedurali specifici di cui al successivo paragrafo, tutti i Destinatari sono pertanto tenuti al rispetto dei principi di comportamento contenuti nei documenti organizzativi al fine di prevenire la commissione dei Reati di cui all'art. 24 bis del Decreto.

3.7.4 Procedure specifiche

Al fine di garantire adeguati presidi nell'ambito delle singole Aree a Rischio, si prevedono qui di seguito le regole che devono essere rispettate dagli Esponenti Aziendali nonché dagli altri soggetti eventualmente autorizzati nell'ambito delle suddette aree.

In particolare:

1) è vietato connettere ai sistemi informatici di Smartest, personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;

2) è vietato in qualunque modo modificare la configurazione software o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;

3) è vietato acquisire, possedere o utilizzare strumenti software o hardware – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software o hardware sianoutilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – chepotrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le Credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);

4) è vietato ottenere Credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate;

5) è vietato divulgare, cedere o condividere con personale interno o esterno a Smartest le proprie Credenziali di accesso ai sistemi e alla rete aziendale, dei clienti o di terze parti;

6) è vietato accedere abusivamente a un sistema informatico altrui o accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;

7) è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, dei clienti o di terze parti, comprensivo di archivi, dati e programmi;

8) è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, dei clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anchenel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

9) è vietato comunicare a persone non autorizzate, interne o esterne a Smartest, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

10) è proibito mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti Virus o altri programmi in grado di danneggiare o intercettare dati;

11) è vietato lo Spamming come pure ogni azione di risposta al medesimo;

12) è vietato inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi.

Smartest si impegna, a sua volta, a porre in essere i seguenti adempimenti:

1) informare adeguatamente i dipendenti, nonché gli altri soggetti eventualmente autorizzati all'utilizzo dei sistemi informativi, dell'importanza di mantenere le proprie Credenziali confidenziali e di non divulgare le stesse a soggetti terzi;

2) prevedere attività di formazione e addestramento periodico in favore dei dipendenti, diversificate in ragione delle rispettive mansioni, nonché in favore degli altri soggetti eventualmente autorizzati all'utilizzo dei sistemi informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;

3) far sottoscrivere ai dipendenti, nonché agli altri soggetti eventualmente autorizzati all'utilizzo dei sistemi informativi, uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;

4) informare i dipendenti, nonché gli altri soggetti eventualmente autorizzati all'utilizzo dei sistemi informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;

5) impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;

6) limitare gli accessi alle stanze server unicamente al personale autorizzato;

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

8) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;

9) impedire l'installazione e l'utilizzo di software non approvati da Smartest e non correlati con l'attività professionale espletata per la stessa;

10) impedire l'installazione e l'utilizzo, sui sistemi informatici di Smartest, di software Peer to Peer mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, Virus, etc.) senza alcuna possibilità di controllo da parte di Smartest;

11) qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a Smartest, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;

12) prevedere un procedimento di autenticazione mediante l'utilizzo di Credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati all'utilizzo dei sistemi informativi;

13) provvedere senza indugio alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale.

3.7.5 Verifiche dell'organo di vigilanza

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui all'art. 24 bis del Decreto sono i seguenti:

- svolgere verifiche periodiche sul rispetto delle procedure adottate e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati di cui all'art. 24 bis del Decreto proponendo eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sui Delitti Informatici, ovvero in occasione di mutamenti nell'organizzazione aziendale e nell'attività in relazione al progresso scientifico e tecnologico;

- proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a Rischio individuate;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

3.8 Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare

3.8.1 Le tipologie di reato

Il D.Lgs. 109/2012 ha ampliato i reati presupposto per la responsabilità amministrativa delle persone giuridiche prevista dal D.Lgs. 231/2001 introducendo norme relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare.

La responsabilità ex D.Lgs. 231 è prevista in presenza delle fattispecie penali di cui all'articolo 2, comma 12-bis, del Testo Unico sull'immigrazione riguardante le ipotesi aggravate del reato in cui incorre il datore di lavoro che occupa, alle proprie dipendenze, lavoratori stranieri privi del permesso di soggiorno, o con permesso scaduto (e del quale non sia stato chiesto, nei termini di legge, il rinnovo) revocato o annullato. Le aggravanti, a fronte delle quali scatterà anche la sanzione ex D.Lgs. 231/2001, riguardano le ipotesi in cui i lavoratori occupati siano: più di tre; minori in età non lavorativa; esposti a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

3.8.2 Aree a rischio

In relazione alla fattispecie di reato in esame le aree ritenute più specificamente a rischio risultano essere le seguenti:

1. Stipulazione di contratti di lavoro subordinato (a tempo indeterminato o determinato), parasubordinato ed autonomo;
2. Acquisti (o altre funzioni eventualmente competenti per), con particolare riferimento alla stipulazione di:

- contratti di somministrazione di lavoro;
- contratti di appalto;
- contratti d'opera.

3.8.3 Principi di comportamento

Predisporre una specifica procedura per l'assunzione di lavoratori stranieri ribadendo che è fatto divieto di impiegare personale violando norme in materia di lavoro.

In particolare è fatto divieto di:

- assumere lavoratori che non siano in regola con il permesso di soggiorno;
- mantenere in servizio personale con il permesso di soggiorno scaduto, revocato o annullato;
- assumere minori in età non lavorativa;
- stipulare contratti di somministrazione, di appalto o d'opera con imprese che impiegano personale non in regola con il permesso di soggiorno.

3.8.4 Procedure specifiche

Al fine di garantire adeguato presidio nell'ambito dell'Area a Rischio, si prevedono qui di seguito le regole che devono essere rispettate dagli Esponenti Aziendali nonché dagli altri soggetti eventualmente autorizzati nell'ambito della suddetta area:

1. osservare la procedura prevista per la stipula di contratti di lavoro subordinato;
2. sottoporre all'approvazione dell'amministratore delegato tutti i contratti riguardanti la stipula di rapporti di lavoro subordinato;
3. osservare la procedura prevista per la stipula di contratti di somministrazione di lavoro, d'opera e di appalto.
4. richiedere ai fornitori o partner commerciali uno specifico impegno al rispetto della normativa in oggetto

3.9 Altri reati

Come evidenziato nell'introduzione del presente Modello, in relazione all'attività svolta dalla Smartest e dall'analisi svolta, è emerso che il rischio relativo alla commissione:

- dei reati di falsità in monete, in carte di pubblico credito e in valori di bollo (art. 25-bis del Decreto);
- dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali e delitti posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9.12.1999 (art.25-quater del Decreto);
- dei reati contro la personalità individuale, contro la vita e l'incolumità individuale (art. 25-quinquies e 25-quater.1 del Decreto);
- dei reati transnazionali (art. 10 L 16.3.2006 n. 146)

appare remoto e, pertanto, solo astrattamente e non concretamente ipotizzabile.

Ne consegue che, almeno per il momento, non si ritiene opportuno prevedere principi di comportamento e controllo ulteriori rispetto alle regole generali di rispetto delle leggi e di correttezza delle operazioni poste in essere.

4 Parte speciale C

4.1 Regolamento di segnalazione all'OdV

Al fine di agevolare l'attività di vigilanza sull'effettività e sull'efficacia del Modello, l'Organismo di Vigilanza è destinatario di tutte le segnalazioni e le informazioni ritenute utili a tale scopo. L'OdV deve trasmettere alla Unità di Compliance di Indra ogni comunicazione che riceve relativa alla perpetrazione delle infrazioni previste dal Decreto o a comportamenti non conformi al Modello.

Tutti i Destinatari del Modello sono tenuti ad informare in modo dettagliato e tempestivo l'Organismo di Vigilanza in ordine ad ogni violazione o sospetto di violazione delModello e dei suoi principi generali, nonché in ordine alla loro inidoneità, inefficacia e a ogni altro aspetto potenzialmente rilevante.

In particolare, i Destinatari sono tenuti a trasmettere tempestivamente all'Organismo di Vigilanza le informazioni concernenti:

- criticità che emergono dall'attività di controllo poste in essere dalle funzioni aziendali addette;
- i provvedimenti o notizie provenienti da qualsiasi Autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D. Lgs. 231/2001;
- le comunicazioni interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di reato di cui al D. Lgs. 231/2001 (ad es.: provvedimenti disciplinari avviati/attuati nei confronti di dipendenti);
- le relazioni o comunicazioni interne dalle quali emergono responsabilità per le ipotesi di reato di cui al D. Lgs. 231/2001;
- le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza - nell'ambito dei procedimenti disciplinari svolti - delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;

- i prospetti riepilogativi dei contratti significativi sottoscritti a seguito di gare, o trattative private con la PA.

Deve essere altresì portata a conoscenza dell'Organismo di Vigilanza ogni altra informazione, di cui si è venuti a diretta conoscenza, proveniente sia dai dipendenti che da terzi, attinente la commissione dei reati previsti dal Decreto o comportamenti non in linea con il Modello predisposto.

Le segnalazioni devono essere effettuate in forma scritta utilizzando l'apposito "Modulo di segnalazione" anche mediante e-mail all'indirizzo: **odv231.smartest@smartest.it**.

L'Organismo di Vigilanza garantisce i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante.

L'Organismo di Vigilanza valuta le segnalazioni ricevute con discrezionalità e responsabilità.

A tal fine, può ascoltare l'autore della segnalazione o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione a non procedere nel solo caso di informativa relativa alla commissione di specifici reati.

Ogni informazione, segnalazione, report, previsti nel presente Modello sono conservati dall'Organismo di Vigilanza in un apposito archivio riservato (informatico o cartaceo) per un periodo di 10 anni.

L'accesso all'archivio è consentito esclusivamente agli Amministratori e al Presidente del Collegio Sindacale, oltre che al componente dell'Organismo di Vigilanza così come alla Unità di Compliance di Indra.

4.2 Facsimile modulo di segnalazione all'OdV

Modulo Segnalazione all'OdV

Segnalazione della commissione o dei tentativi di commissione di uno dei reati contemplati dal Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300", ovvero della violazione o dell'elusione fraudolenta del Modello di Organizzazione, Gestione e Controllo e/o del Codice Etico.

AUTORE DEL COMPORTAMENTO OGGETTO DELLA SEGNALAZIONE _____ ____

DESCRIZIONE DI DETTAGLIO DEL COMPORTAMENTO CHE ORIGINA LA SEGNALAZIONE:

DATI DEL SEGNALANTE (IN CASO DI SEGNALAZIONE NON ANONIMA)
Nome:
Cognome:
Unità Organizzativa:
Telefono:
E-Mail: _____

Data Firma

Informativa ai sensi dell'art. 13 D.Lgs. 196/2003

Smartest S.r.l. unipersonale con sede legale in Castelfranco Veneto ,Piazza della Serenissima n. 80, titolare del trattamento dei dati personali, ai sensi dell'art. 13 del D.lgs. 196/2003 rende noto che i Suoi dati personali acquisiti mediante la presente segnalazione saranno trattati esclusivamente per finalità connesse al rispetto degli obblighi derivanti dal D.Lgs. 231/2001, nonché utilizzati, ed in seguito conservati, prevalentemente in forma cartacea. Riconosciuta la legittimità anche di segnalazioni "anonime", il conferimento dei suoi dati appare facoltativo ed un suo rifiuto in tal senso non comporterà nessuna conseguenza circa la validità dell'operato dell'Organismo di Vigilanza di Smartest (di qui in avanti più semplicemente O.d.V.). Il segnalante resta, in ogni caso, personalmente responsabile dell'eventuale contenuto diffamatorio delle proprie comunicazioni e Smartest mediante il proprio O.d.V., si riserva il diritto di non prendere in considerazione le segnalazioni prodotte in evidente "mala fede". Smartest ricorda, inoltre, che i dati da Lei forniti devono essere pertinenti rispetto alle finalità della segnalazione, cosicché l'O.d.V. sarà libero di non dare seguito alle segnalazioni riguardanti condotte o soggetti estranei agli obblighi derivanti dal D.Lgs. 231/2001. Salvo l'espletamento di obblighi derivanti dalla legge, i dati personali da Lei forniti non avranno alcun ambito di comunicazione e diffusione. Ai sensi dell'art. 7 del D.Lgs. 196/2003 Lei potrà esercitare i seguenti diritti:

- ottenere indicazione dell'origine dei Suoi dati nonché delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del titolare e dei responsabili nonché dei soggetti o delle categorie di soggetti ai quali i dati personali potranno essere comunicati;
- ottenere l'aggiornamento, la rettificazione ovvero, quando ne ha interesse, l'integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non e' necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; l'attestazione delle operazioni che sono state portate a conoscenza di terzi, anche per quanto riguarda il loro contenuto; di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
- opporsi, in tutto o in parte, per motivi legittimi al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta.

Per l'esercizio dei succitati diritti, Lei potrà rivolgersi direttamente all'O.d.V. Responsabile del trattamento a ciò designato dal Titolare ai sensi dell'art. 29 del D.Lgs. 196/2003, tramite casella di posta elettronica o, tramite posta ordinaria presso l'Organismo di Vigilanza c/o Smartest S.r.l. presso la sede legale, le unità operative della società o dell'O.d.V.