

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ex Decreto Legislativo 8 giugno 2001 n. 231

INDICE

Parte generale

- 1.** La responsabilità amministrativa a carico delle persone giuridiche
 - 1.1 Il Decreto Legislativo n. 231/2001
 - 1.2 L'adozione del "Modello di organizzazione, gestione e controllo" quale possibile esimente della responsabilità amministrativa
- 2.** Adozione del Modello da parte di ADP Dealer Services Italia S.r.l.
 - 2.1 Obiettivi perseguiti da ADP Dealer Services Italia s.r.l con l'adozione del Modello
 - 2.2 Funzione del Modello
 - 2.3 Struttura del Modello: parte generale e parti speciali in relazione alle diverse tipologie di reati da prevenire
 - 2.4 I principi ispiratori del Modello
 - 2.5 Recepimento, modifiche e integrazioni del Modello
- 3.** Organismo di Vigilanza (OdV)
 - 3.1 Identificazione dell'OdV
 - 3.2 Funzione e poteri dell'OdV

- 3.3 Flussi informativi nei confronti dell'OdV
- 3.4 Reporting nei confronti degli organi societari
- 3.5 Regolamento operativo dell'OdV
- 3.6 Cause di revoca e di ineleggibilità dei membri dell'OdV
- 4. Sanzioni disciplinari
 - 4.1 Principi generali
 - 4.2 Sanzioni e misure nei confronti dei dipendenti
 - 4.3 Sanzioni e misure nei confronti dei dirigenti
 - 4.4 Misure nei confronti di amministratori e sindaci
 - 4.5 Misure nei confronti di collaboratori esterni e partner
- 5. Modello e Codice Etico
- 6. Il Modello organizzativo di ADP Dealer Services Italia s.r.l: costruzione, principi e struttura
- 7. Formazione e diffusione del Modello
 - 7.1 Formazione ed informazione dei Dipendenti
 - 7.2 Selezione ed informazione dei Consulenti e dei Partner

- Parte speciale 1 Reati societari e il riciclaggio
- Parte speciale 2 Reati colposi
- Parte speciale 3 Reati informatici

Parte speciale 4 Reati contro la P.A.

Parte speciale 5 Reati ambientali

1. La responsabilità amministrativa a carico delle persone giuridiche

1.1 Il Decreto Legislativo n. 231/2001

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all’art. 11 della legge 29 settembre 2000 n. 300 – il D.Lgs 231/2001, entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l’Italia ha già da tempo aderito, quali la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Con tale Decreto, dal titolo “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica” (definite dalla legge come “Enti” o “Ente”), è stato introdotto nell’ordinamento italiano un regime di responsabilità amministrativa (riferibile sostanzialmente alla responsabilità penale) a carico degli Enti per alcuni reati commessi, nell’interesse o vantaggio degli stessi, (i) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi, nonché (ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Tale responsabilità si

aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

L'ampliamento della responsabilità mira a coinvolgere gli Enti nella punizione di taluni reati commessi nel loro interesse o a loro vantaggio. Tra le sanzioni previste, le più gravi sono rappresentate da misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la P.A., l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi.

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

Quanto alla tipologia di reati destinati a comportare il suddetto regime di responsabilità amministrativa a carico degli Enti, il Decreto – nel suo testo originario – si riferisce ad una serie di reati commessi nei rapporti con la Pubblica Amministrazione e precisamente:

- indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316-ter cod. pen.);
- concussione (art. 317 cod. pen.);
- corruzione per un atto d'ufficio (art. 318 cod. pen.);
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 cod. pen.);
- corruzione in atti giudiziari (art. 319-ter cod. pen.);
- istigazione alla corruzione art. 322 cod. pen.);

- truffa in danno dello Stato o di altro Ente pubblico (art. 640, comma primo, n. 1 cod. pen.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* cod. pen.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640-*ter* cod. pen.).

Successivamente, l'art. 6 della legge 23 novembre 2001 n. 409, recante "Disposizioni urgenti in vista dell'introduzione dell'euro" ha inserito nell'ambito del Decreto l'art. 25-*bis*, che mira a punire il reato di "falsità in monete, in carte di pubblico credito e in valori di bollo".

In seguito, l'art. 3 del Decreto Legislativo 11 aprile 2002 n. 61, in vigore dal 16 aprile 2002, nell'ambito della riforma del diritto societario, ha introdotto il nuovo art. **25-*ter*** del D.Lvo. 231/2001, estendendo il regime di responsabilità amministrativa degli Enti anche ai c.d. reati societari, così come configurati dallo stesso Decreto n. 61/2002 (false comunicazioni sociali, false comunicazioni sociali in danno dei soci o dei creditori, falso in prospetto, falsità nelle relazioni o nelle comunicazioni della società di revisione, impedito controllo, indebita restituzione dei conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori, formazione fittizia del capitale, indebita ripartizione dei beni sociali da parte dei liquidatori, illecita influenza sull'assemblea, agiotaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza).

In seguito, l'art. 3 della L. 14 gennaio 2003, n. 7 ha introdotto l'art. **25-quater**, il quale dispone la punibilità dell'Ente per i delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali. Mentre l'art. **25-quinquies**, introdotto dall'art. 5 della l. 11 agosto 2003, n. 228 ha esteso la responsabilità amministrativa dell'Ente ai reati contro la personalità individuale.

L'art. 9 della L. 18 aprile 2005, n. 62 (di seguito la “Legge Comunitaria 2004”) ha, inoltre, inserito l'art. **25-sexies** volto ad estendere la responsabilità amministrativa degli Enti ai nuovi reati di abuso di informazioni privilegiate e di manipolazione del mercato.

La legge Comunitaria 2004 ha, inoltre, modificato il TUF introducendo una specifica disposizione, l'art. 187-*quinquies*, ai sensi della quale l'Ente è responsabile del pagamento di una somma pari all'importo della sanzione amministrativa irrogata per gli illeciti amministrativi di abuso di informazioni privilegiate (art. 187-*bis* TUF) e di manipolazione del mercato (art. 187-*ter* TUF) commessi nel suo interesse o a suo vantaggio da: a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria o funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

La Legge 28 dicembre 2005, n. 262 (“Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari”) ha integrato e modificato sia il TUF sia il Codice Civile, introducendo, tra l'altro, il nuovo art. 2626-*bis* cod. civ. relativo al reato di “Omessa comunicazione del conflitto di interessi”. Tale reato è stato introdotto, ad opera della medesima legge n. 262/2005, nell'art. 25-*ter* del D.Lvo. 231/2001.

Ulteriori modifiche legislative in materia di responsabilità degli enti sono state introdotte dalla Legge n. 7/2006 che vieta e punisce le così dette pratiche di infibulazione (art. 583-*bis* c.p.), dalla Legge n. 38/2006 contenente “*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*” (artt. 600-*ter* e 600-*quater* c.p.) includendo anche le ipotesi in cui il materiale pornografico utilizzato rappresenti immagini virtuali di minori (c.d. pedopornografia virtuale) e, infine, dalla Legge n. 146/2006 che ha stabilito la responsabilità *ex* 231 per gli illeciti amministrativi dipendenti dai delitti di associazione a delinquere, riciclaggio e impiego di denaro e beni di provenienza illecita, traffico di migranti e intralcio alla giustizia aventi carattere di transnazionalità.

La Legge 123/2007, oltre ad aver abrogato la previsione relativa ai reati di riciclaggio e impiego di denaro e beni di provenienza illecita aventi carattere di transnazionalità, ha introdotto l’art. 25-*septies* che ha ulteriormente esteso l’ambito di applicazione della responsabilità amministrativa degli enti ai reati di omicidio colposo e lesioni colpose gravi o gravissime che si verificano in connessione alla violazione delle norme per la prevenzione degli infortuni sul lavoro o relative alla tutela dell’igiene e della salute sul lavoro (artt. 589 e 590, comma III, c.p.).

La Legge 231/2007 ha introdotto la punibilità dell’ente per i reati di ricettazione, riciclaggio e impiego di capitali illeciti, anche se compiuti in ambito prettamente nazionale sempre che ne derivi un interesse o un vantaggio per l’ente medesimo.

Da ultimo, l’art. 7 della Legge n. 48/2008 sulla criminalità informatica ha introdotto l’art. 24-*bis* che prevede la responsabilità dell’ente in relazione ai delitti informatici ed al trattamento illecito di dati (artt. 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*, 615-*quater* e 615-*quinquies* c.p.).

1.1 L'adozione del “Modello di organizzazione e di gestione” quale possibile esimente dalla responsabilità amministrativa

L'articolo 6 del Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede, tuttavia, una forma specifica di esonero da detta responsabilità qualora l'Ente dimostri che:

- a) l'organo dirigente dell'Ente ha adottato ed efficacemente attuato, prima della commissione del fatto, Modelli di organizzazione e di gestione idonei a prevenire i Reati e gli Illeciti della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e sull'osservanza dei Modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo c.d. Organismo di Vigilanza (OdV);
- c) le persone che hanno commesso i Reati e gli illeciti hanno agito eludendo fraudolentemente i suddetti Modelli;
- d) non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Il Decreto prevede, inoltre, che – in relazione all'estensione dei poteri delegati e al rischio di commissione degli illeciti – i Modelli di cui alla lettera a) debbano rispondere alle seguenti esigenze:

1. individuare le attività nel cui ambito esiste la possibilità che vengano commessi i Reati e gli illeciti;

2. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai Reati e agli illeciti;
3. individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali Reati ed illeciti;
4. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
5. introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

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

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

2. Adozione del Modello da parte di ADP Dealer Services Italia S.r.l.

2.1 Obiettivi perseguiti da ADP Dealer Services Italia s.r.l con l'adozione del Modello

ADP Dealer Services Italia s.r.l. è una società, appartenente al gruppo multinazionale Automatic Data Processing Inc. - con sede a Roseland, New jersey, USA - direttamente posseduta da ADP NEDERLAND B.V. e da ADP INTERNATIONAL B.V., leader nel mercato italiano del software per il settore automotive: i suoi clienti sono importanti

Società produttrici di automobili, associazioni di concessionari e concessionari, distributori di ricambi e rivenditori di automobili, officine autorizzate e indipendenti. La società, che conta al 31/08/2010 172 dipendenti, è stata fondata nel 1969 e nell'ultimo esercizio (fiscal year 2010, chiuso al 30/06/2010) ha fatturato 20,27 milioni di €.

La sede legale è a Milano, in via Montenapoleone 21, mentre la sede operativa è a Vigonza (PD), via Julia 39.

ADP Dealer Services s.r.l., società assoggettata alla direzione ed al coordinamento di "Automatic Data Processing Inc." ex art. 2497 bis. c.c., ha un sistema di amministrazione e controllo pluripersonale e collegiale ed è, pertanto, amministrata da un Consiglio di Amministrazione formato da quattro membri, come da certificato della Camera di Commercio in data 10 gennaio 2008 che si allega sub 1).

La legale rappresentanza è attribuita al Presidente ed all'Amministratore Delegato, ampie deleghe sono altresì conferite al Direttore Generale.

E' presente un Collegio Sindacale composto da 5 membri (presidente e 2 effettivi più 2 supplenti) come da certificato camerale già allegato.

Il bilancio della società, sebbene non vi sia l'obbligo giuridico, viene comunque certificato dalla società Deloitte & Touche LLP.

Il sistema organizzativo di ADP Dealer Services Italia s.r.l. è adeguatamente organizzato e chiaro quanto all'attribuzione di responsabilità ed alle linee di dipendenza gerarchica: tutte le mansioni aziendali sono definite da un articolato organigramma che si allega sub 2) e si richiama quale parte integrante del presente Modello Organizzativo.

Inoltre ADP Dealer Services già da tempo ha adottato un ampio sistema di procedure aziendali assai puntuali a cura e sotto la responsabilità del Direttore Finanza ed

Amministrazione e del Direttore delle Risorse Umane che si allegano sub 3) e che parimenti si richiamano quali parti integranti del Modello:

- Normativa emissione procedure (all. 3.1);
- Gestione dei crediti (all. 3.2);
- Emissione accrediti (all. 3.3);
- Acquisti (all. 3.4);
- Investimenti (all. 3.5);
- Cassa (all. 3.6);
- Normativa generale e specifica sul sistema di incentivazione (all. 3.7);
- Trasferte (all. 3.8);
- Assegnazione beni aziendali (all. 3.9);
- Utilizzo telefoni cellulari (all. 3.10);
- Richieste di assunzione (all. 3.11);
- Procedura di bilancio (all. 3.12);
- Procedura sicurezza informatica (all. 3.13);
- Documento programmatico sulla sicurezza dati (all. 3.14);
- Procedura sicurezza (all. 3.15);
- Procedura emergenza (all. 3.16).

In forza di tali procedure viene garantita l'applicazione del principio della separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione deve essere sotto la responsabilità di persona diversa da chi contabilizza, segue operativamente o controlla

l'operazione: nessuno può gestire in autonomia un intero processo. D'altra parte i poteri autorizzativi e di firma appaiono coerenti con le responsabilità assegnate.

Tuttavia ADP Dealer Services Italia S.r.l. – sensibile all'esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria immagine e del lavoro dei propri dipendenti – ha ritenuto conforme alle proprie politiche aziendali procedere all'attuazione del Modello Organizzativo.

Tale iniziativa, che fa seguito all'emanazione del Codice etico, è stata assunta nella convinzione che l'adozione di tale Modello – al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio – possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto di ADP Dealer Services Italia s.r.l, affinché seguano, nell'espletamento delle proprie attività, dei comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei Reati e degli illeciti.

Il suddetto Modello è stato predisposto dalla società tenendo presenti, oltre alle prescrizioni del Decreto e del TUF, le Linee Guida elaborate da Confindustria aggiornate al 31 marzo 2008.

Il presente Modello è stato adottato dal Consiglio di Amministrazione di ADP Dealer Services Italia S.r.l. con delibera del 3/10/2008 e aggiornato il 13/09/2010 con approvazione dell'Amministratore Delegato.

Sempre in attuazione di quanto previsto dal Decreto, il Consiglio di Amministrazione di ADP Dealer Services Italia S.r.l., nel varare il suddetto Modello, ha affidato l'incarico di Organismo di Vigilanza ad un collegio composto da un membro interno, e due membri esterni.

Il membro interno , con riferimento a tale sua funzione di componente dell'Organismo di Vigilanza, sarà indipendente dalla struttura gerarchica aziendale.

2.2 Funzione del Modello

Scopo del Modello è la costruzione di un sistema strutturato e organico di procedure nonché di attività di controllo, da svolgersi anche in via preventiva (controllo *ex ante*), volto a prevenire la commissione dei Reati e degli illeciti.

In particolare, mediante l'individuazione delle Aree a Rischio e la loro conseguente proceduralizzazione, il Modello si propone come finalità quelle di:

- determinare, in tutti coloro che operano in nome e per conto di ADP Dealer Services Italia s.r.l, soprattutto nelle medesime Aree a Rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti di ADP Dealer Services Italia s.r.l;
- ribadire che tali forme di comportamento illecito sono fortemente condannate da ADP Dealer Services Italia s.r.l in quanto (anche nel caso in cui ADP Dealer Services Italia s.r.l fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico – sociali cui intende attenersi nell'espletamento della propria missione aziendale;
- consentire ad ADP Dealer Services Italia s.r.l, grazie ad un'azione di monitoraggio sulle Aree a Rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati e più in generale degli illeciti.

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

- l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- la mappa delle Aree a Rischio del Gruppo;
- l'attribuzione all'OdV di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- la verifica e documentazione delle operazioni a rischio;
- il rispetto del principio della separazione delle funzioni;
- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la verifica dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico (controllo *ex post*).

2.3 Struttura del Modello: Parte Generale e Parti Speciali in funzione delle diverse fattispecie di Reati e di illeciti da prevenire

Il presente Modello è costituito da una "Parte Generale" e da singole "Parti Speciali" predisposte per le diverse tipologie di Reati e di illeciti da prevenire.

E' demandato al Consiglio di Amministrazione, su indicazione e secondo le opportune modalità indicate dall'Organismo di Vigilanza, di integrare il presente Modello, mediante apposita delibera, con ulteriori Parti Speciali relative ad altre tipologie di reati o di illeciti amministrativi che, per effetto di altre normative, risultino inserite o comunque collegate all'ambito di applicazione del Decreto.

2.4 I principi ispiratori del Modello

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo esistenti e già operanti nella Società, rilevati in fase di analisi delle attività a rischio, in quanto idonei a valere anche come misure di prevenzione dei Reati e degli illeciti e di controllo sui processi coinvolti nelle Aree a Rischio.

Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali ed effettuare i controlli sull'attività di impresa, anche in relazione ai Reati e agli illeciti da prevenire, il Gruppo ha individuato:

- 1) il Codice etico;
- 2) il sistema di procedure interne e di reporting alla casa madre;
- 3) il sistema sanzionatorio di cui al CCNL metalmeccanici applicabile;
- 4) documento della sicurezza aggiornato al nuovo Testo Unico (D.Lvo 09/04/2008 n. 81).

Le regole, le procedure e i principi di cui agli strumenti sopra elencati che non vengono riportati espressamente nel presente Modello, fanno comunque parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare e che tutti i Destinatari sono tenuti a rispettare. Le statuizioni contenute nel presente modello, in ogni caso, prevalgono su eventuali disposizioni contrastanti contenute in diverse procedure aziendali.

Il personale interessato deve essere periodicamente aggiornato sulle procedure aziendali adottate per la prevenzione dei Reati e degli illeciti nonché sull'evoluzione della relativa normativa.

2.5 Recepimento, modifiche e integrazioni del modello

Essendo il presente Modello un “atto di emanazione dell'organo dirigente” (in conformità alle prescrizioni dell'art. 6, comma primo, lett. a del Decreto) le successive

modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza del Consiglio di Amministrazione di ADP Dealer Services Italia S.r.l.

E' peraltro riconosciuta all'Amministratore Delegato di ADP Dealer Services Italia S.r.l. e/o al Direttore Generale la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere formale.

ADP Dealer Services Italia s.r.l., come già precisato, ha già un articolato sistema di procedure aziendali che viene integralmente richiamato e diviene parte integrante del Modello Organizzativo.

Tale sistema prevede anche una Normativa di emissione delle procedure aziendali che ha come obiettivo la regolamentazione, la manutenzione programmata e gestione del flusso delle procedure in azienda.

A tal fine è stato istituito un Comitato Procedure di cui sono membri l'Amministratore Delegato e/o il Direttore generale, il Direttore HR e il Direttore F&A.

Naturalmente la normativa di emissione delle procedure aziendali deve ora integrarsi con i principi del D. Lgs. 231/01.

Pertanto ogni modifica delle procedure di natura sostanziale d'ora in avanti sarà adottata non dalla Direzione Generale, bensì dal Consiglio di Amministrazione su proposta del Comitato Procedure, previo parere favorevole dell'OdV.

La manutenzione delle procedure - l' *upgrade* delle procedure - continuerà ad avvenire su base semestrale e sarà promossa dal Comitato Procedure, eventualmente dietro segnalazione delle Direzioni dell'Azienda: ogni modifica od integrazione - sempre che non si tratti di modifiche aventi natura sostanziale - dovrà essere approvata dalla Direzione Generale su proposta del Comitato Procedure, previo parere favorevole dell'OdV.

Infine, l'Organismo di Vigilanza, ha la facoltà di proporre al Consiglio di Amministrazione e all'Amministratore Delegato eventuali modifiche delle Aree a Rischio e/o altre integrazioni o aggiornamenti del presente Modello.

A seconda del tipo di modifica proposta, essa sarà apportata direttamente dall'Amministratore Delegato o da questi sottoposta all'approvazione del Consiglio di Amministrazione di ADP Dealer Services Italia S.r.l..

3. Organismo di Vigilanza (OdV)

3.1 Identificazione dell'Organismo di Vigilanza (OdV)

L'art. 6, comma primo, lett. b, del citato D. Lgs. 231/01, pone come condizione, per la concessione dell'esimente dalla responsabilità amministrativa, che sia affidato ad un organismo dell'Ente dotato di autonomi poteri, di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei Modelli nonché di curarne l'aggiornamento: tale organismo deve essere caratterizzato da autonomia, indipendenza, professionalità e continuità d'azione, come previsto nelle Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex. D. Lgs. 231/01, emanate da Confindustria.

In attuazione di quanto previsto dal Decreto è stato individuato nell'ambito di ADP Dealer Services Italia s.r.l come soggetto più idoneo ad assumere detto compito un organismo collegiale composto da un membro interno e da due membri esterni come più sopra specificato.

3.2 Funzioni e poteri dell'OdV

All'OdV di ADP Dealer Services Italia s.r.l è affidato sul piano generale il compito di vigilare:

- a) sull'osservanza delle prescrizioni del Modello da parte di tutti i destinatari del medesimo;
- b) sulla reale efficacia ed effettiva capacità del Modello, in relazione alla struttura aziendale, di prevenire la commissione di Reati e di illeciti;
- c) sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali ovvero all'emanazione di nuove norme integrative o modificative del Decreto.

Sul piano più operativo è affidato all'OdV di ADP Dealer Services Italia s.r.l il compito di:

- attivare le procedure di controllo, tenendo presente che una responsabilità primaria sul controllo delle attività, anche per quelle relative alle Aree a Rischio, resta comunque demandata al management operativo e forma parte integrante del processo aziendale ("controllo di linea") – il che conferma l'importanza di un processo formativo del personale;
- condurre periodiche ricognizioni dell'attività aziendale ai fini della mappatura aggiornata delle Aree a Rischio nell'ambito del contesto aziendale;
- effettuare periodicamente verifiche - anche a sorpresa - mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle Aree a Rischio come definite nelle singole Parti Speciali del Modello;

promuovere idonee iniziative per la diffusione, la conoscenza e la comprensione del Modello e proporre la predisposizione della documentazione organizzativa interna necessaria al fine del funzionamento del Modello stesso contenente istruzioni, chiarimenti o aggiornamenti;

- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere allo stesso OdV obbligatoriamente trasmesse o tenute a sua disposizione;
- coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle Aree a Rischio. A tal fine, l'OdV viene tenuto costantemente informato sull'evoluzione delle attività nelle suddette Aree a Rischio ed ha libero accesso a tutta la documentazione aziendale rilevante. All'OdV devono essere inoltre segnalate da parte del management eventuali situazioni dell'attività aziendale che possano esporre il Gruppo al rischio di illeciti;
- controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto nelle singole Parti Speciali del Modello per le diverse tipologie di illeciti. In particolare all'OdV devono essere segnalate le attività più significative o le operazioni contemplate dalle Parti Speciali, devono essere messi a sua disposizione i dati di aggiornamento della documentazione, al fine di consentire l'effettuazione dei controlli;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;

verificare che gli elementi previsti dalle singole Parti Speciali del Modello per le diverse tipologie di illeciti (adozione di clausole standard, espletamento di procedure, ecc.) siano sempre adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, proponendone, in caso contrario, un aggiornamento; coordinarsi con i responsabili delle altre funzioni aziendali ed eventualmente con consulenti esterni appositamente incaricati per i diversi aspetti attinenti all'attuazione del Modello (definizione di clausole standard, formazione del personale, provvedimenti disciplinari, ecc.);

- verificare – con il supporto delle altre funzioni aziendali competenti – il sistema di poteri in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti a Manager Aziendali;
- verificare periodicamente, con il supporto delle altre funzioni competenti ed eventualmente di consulenti esterni, la validità delle clausole standard finalizzate all’attuazione di meccanismi sanzionatori (quali il recesso dal contratto nei riguardi di Partner, Consulenti o Fornitori) qualora si accertino violazioni delle prescrizioni;
- segnalare prontamente al Consiglio di Amministrazione ed al Collegio Sindacale ogni rilevante operazione anomala adottata in via straordinaria e per la quale non è prevista una specifica procedura;
- promuovere, gestire ed organizzare, unitamente alla Direzione del personale, corsi di formazione che eventualmente prevedano interventi mirati a seconda della collocazione aziendale dei destinatari e del fatto che essi operino in specifiche Aree di Rischio (ad esempio formazione on line, formazione rivolta ai neo-quadri, formazione per i neo-assunti con contestuale analisi delle problematiche riguardanti il Decreto).

I compiti di vigilanza dell'OdV in relazione all’osservanza del Modello per quanto concerne i reati commessi in violazione delle norme antinfortunistiche sono i seguenti:

1. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati commessi in violazione delle norme antinfortunistiche (*follow up*). Con riferimento a tale punto l'OdV - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia in possesso di requisiti formativi e professionali pari a quelli del RSPP che assicurino l’obiettività e l’imparzialità, nonché l’indipendenza dal settore di lavoro sottoposto a verifica ispettiva - condurrà una periodica attività di analisi sulla funzionalità

del sistema preventivo adottato e proporrà ai soggetti competenti della Società eventuali azioni migliorative ovvero aggiornamenti;

2. proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

3. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;

Allo scopo di svolgere i propri compiti, l'OdV può:

a) partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;

b) accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

Quanto all'indipendenza ed alla autonomia dell'OdV di ADP Dealer Services Italia s.r.l si prevede che:

1. le attività poste in essere dall'OdV non possono essere sindacate da alcun organismo o struttura aziendale, fermo restando però che l'organo dirigente è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto all'organo dirigente appunto rimonta la responsabilità ultima del funzionamento (e dell'efficacia) del Modello organizzativo;

2. l'OdV deve avere libero accesso presso tutte le funzioni della Società – senza necessità di alcun consenso preventivo o preavviso – onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dai D.Lgs. n. 231/2001;

3. nel contesto delle procedure di formazione del budget aziendale, l'organo dirigente dovrà approvare una dotazione adeguata di risorse finanziarie a disposizione dell'OdV, eventualmente su proposta dell'OdV stesso, di cui tale organo potrà disporre in totale autonomia per ogni esigenza necessaria al corretto svolgimento delle proprie funzioni (es. consulenze specialistiche, trasferte, ecc.).

3.3 Flussi informativi nei confronti dell'OdV

In ambito aziendale dovrà essere portata a conoscenza dell'OdV, oltre alla documentazione prescritta nelle singole Parti Speciali del Modello secondo le procedure ivi contemplate, ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi ed attinente all'attuazione del Modello nelle Aree a Rischio.

In particolare, dipendenti, dirigenti e amministratori sono tenuti a riferire all'OdV notizie rilevanti e relative alla vita della società nella misura in cui esse possano esporre la Società al rischio di Reati e di illeciti ovvero comportare violazioni del Modello, e notizie relative al mancato rispetto delle regole contenute nel Modello o alla consumazione di qualsiasi reato o illecito.

Valgono al riguardo le seguenti prescrizioni:

- nell'ambito delle Aree a Rischio le funzioni coinvolte in qualsiasi attività di natura ispettiva da parte di organismi pubblici (Magistratura, Guardia di Finanza, altre Autorità, ecc.) dovranno informare l'OdV dell'avvio di questi interventi;
- devono essere raccolte e trasmesse all'OdV eventuali segnalazioni relative alla commissione di illeciti o di comportamenti in violazione del Modello o comunque a comportamenti non in linea con le regole di condotta ed i principi di cui al Codice Etico;

- l'OdV avrà libero accesso alla reportistica periodica in materia di salute e sicurezza sul lavoro oltre e dovrà essergli inviata la documentazione completa in caso di infortuni anche di lievissima entità che si dovessero verificare in azienda;
- l'OdV valuterà le segnalazioni ricevute e gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere a una indagine interna; le eventuali sanzioni disciplinari che l'OdV riterrà di dover assumere dovranno essere trasmesse al General Manager ed al Consiglio di amministrazione i quali, previa autonoma valutazione, ne daranno attuazione secondo la normativa vigente; in caso di dubbi sulla correttezza di comportamenti di Consulenti, Partner o Fornitori, l'OdV ne darà comunicazione all'Amministratore Delegato per una autonoma valutazione;
- le segnalazioni all'OdV potranno essere in forma scritta o orale ed avere ad oggetto ogni violazione o sospetto di violazione del Modello o di regola di comportamento prevista dal Codice Etico. L'OdV agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone accusate erroneamente e/o in mala fede;
- per maggiore tutela dei segnalanti è prevista la possibilità di trasmettere le violazioni di cui al punto precedente, anche in forma anonima, direttamente presso la sede operativa della società ADP Dealer Services Italia Srl - sita in via Julia n. 39, 35010 Vigonza (Padova) - all'attenzione del Responsabile del Servizio di Prevenzione e Protezione.

Oltre alle segnalazioni di cui sopra, i dipendenti devono obbligatoriamente e immediatamente trasmettere all'OdV le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini per i reati previsti dal Decreto 231/01, anche nei confronti di ignoti, qualora tali indagini coinvolgano la società o suoi dipendenti o organi societari;
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario per i suddetti reati;
- tutti i rapporti aziendali dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.L.vo 231/01;
- le notizie relative ai procedimenti sanzionatori svolti e alle eventuali misure irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, sempre qualora siano legati alla commissione dei reati previsti dal Decreto 231/01 o alla violazione delle regole di comportamento o procedurali del Modello.

Gli obblighi di segnalazione da parte di Consulenti e Partner saranno specificati in apposite clausole inserite nei contratti che legano tali soggetti ad ADP Dealer Services Italia s.r.l.

Ogni informazione, segnalazione, report previsti nel presente Modello sono conservati dall'OdV in un apposito database per un periodo di almeno 10 anni.

L'accesso a tale database è consentito esclusivamente ai membri del Collegio Sindacale e al personale appositamente delegato dall'OdV.

3.4 Reporting nei confronti degli organi societari

L'OdV ha tre linee di *reporting*:

- la prima, su base continuativa, nei confronti dell'Amministratore Delegato;
- la seconda, su base annua, nei confronti del Consiglio di Amministrazione;
- la terza, sempre su base annua, nei confronti del Collegio Sindacale.

I report dell'OdV hanno ad oggetto l'attività svolta dall'Ufficio per l'attuazione e l'efficacia del Modello, la segnalazione di eventuali criticità emerse e le proposte per il miglioramento e l'implementazione del Modello.

Gli incontri con gli organi cui l'OdV riferisce devono essere verbalizzati e copie di tali verbali devono essere custodite dall'OdV e dagli organismi di volta in volta coinvolti.

L'OdV potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione o dal Collegio Sindacale e potrà a sua volta presentare richiesta in tal senso.

3.5 Regolamento operativo dell'OdV

L'OdV si riunisce su richiesta del proprio Presidente, oppure quando ne facciano richiesta scritta almeno due componenti dell'Organismo, oppure quando ne facciano richiesta scritta il Presidente del Consiglio di Amministrazione e/o il Presidente del Collegio Sindacale.

Si raccomanda all'OdV di riunirsi almeno due volte per anno, con cadenza indicativa semestrale.

Le riunioni dell'OdV sono convocate dal Presidente mediante avviso contenente l'indicazione della data, del luogo, dell'ora della riunione e del relativo ordine del giorno; l'avviso deve essere inviato a tutti i componenti dell'OdV - anche per posta elettronica - almeno tre giorni prima della data stabilita per la riunione o, in caso di urgenza, almeno un giorno prima.

Si intende in ogni caso validamente convocata la riunione alla quale, pur in assenza di formale convocazione, partecipino tutti i componenti dell'OdV.

Le riunioni dell'OdV sono valide con la presenza della maggioranza dei componenti.

In caso di impedimento del Presidente, le funzioni di presidenza della riunione sono svolte dal componente anagraficamente più anziano.

I singoli componenti dell'OdV possono partecipare alle riunioni in audio / videoconferenza. La riunione si intende in tal caso tenuta nel luogo dove si trova il Presidente, che ha l'obbligo di accertarsi che i partecipanti collegati in audio / videoconferenza abbiano la possibilità di prendere parte attiva ai lavori della riunione.

L'OdV delibera a maggioranza dei presenti.

Del contenuto delle riunioni e delle decisioni assunte si dà atto a verbale; il verbale è redatto da chi presiede la riunione.

I verbali sono riportati su apposito libro dell'OdV e sono firmati da tutti i presenti.

3.6 Cause di revoca e di ineleggibilità dei membri dell'OdV

I membri dell'O.d.V vengono nominati dal C.d.A. rimangono in carica per tre anni e sono, in linea di principio, irrevocabili.

Chi svolge le funzioni di Organismo di Vigilanza deve essere revocato, con provvedimento del Consiglio di Amministrazione adeguatamente motivato, esclusivamente nei seguenti casi:

1. in caso di inadempienze reiterate ai suoi compiti o inattività ingiustificata (in particolare per mancato aggiornamento del Modello quando ricorrono acquisizioni, dismissioni, fusioni e scissioni, nonché trasformazioni della Società, nonché nel caso di modifiche e integrazioni del decreto 231/01 e/o della normativa di riferimento);

2. nel caso in cui alla Società vengano irrogate sanzioni interdittive a causa dell'inattività dello stesso;
3. quando, in caso di riscontrate violazioni del Modello da parte dei soggetti obbligati, non provveda puntualmente a riferire della violazione, dell'inidoneità e/o dell'inefficace attuazione del Modello;
4. nel caso in cui sia coniuge, parente o affine entro il secondo grado, ovvero socio in affari, di qualunque dei soggetti sottoposti al suo controllo, nonché abbia interessi in comune o in contrasto con gli stessi;
5. nel caso in cui svolga attività e/o incarichi di rappresentanza della Società sottoposta al suo controllo, o semplicemente in contrasto con essa, ovvero sia titolare di deleghe o di procure speciali per l'amministrazione della società stessa;
6. qualora il membro dell'Organismo di Vigilanza sia sindaco supplente della società e tale carica diventi "effettiva";
7. qualora venga condannato, con sentenza passata in giudicato, anche ai sensi dell'art. 444 c.p.p., per fatti connessi allo svolgimento del suo incarico ovvero abbia un qualsiasi carico pendente per qualsiasi reato;
8. qualora venga dichiarato interdetto, inabilitato nonché fallito, ovvero sia condannato dall'Autorità Giudiziaria con sentenze che comportino l'interdizione dai Pubblici Uffici, dagli uffici direttivi delle imprese e delle persone giuridiche, da una professione o da un'arte, nonché comporti l'incapacità di contrattare con la Pubblica Amministrazione;

I casi di revoca di cui ai punti 4,5,6, 7 e 8 costituiscono anche causa di ineleggibilità a tale ufficio.

Tutti i membri dell'Organismo di Vigilanza devono presentare annualmente al Consiglio di Amministrazione una dichiarazione scritta con cui attestano l'idoneità alla prosecuzione del mandato.

Qualora uno o più membri dell'OdV vengano revocati per i motivi più sopra specificati, dovrà essere immediatamente nominato un nuovo membro dal CdA.

4. Sanzioni disciplinari

4.1 Principi generali

Aspetto essenziale per l'effettività del Modello è costituito dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposta ai fini della prevenzione dei reati e degli illeciti in generale, delle procedure interne 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 dalla società in piena autonomia, indipendentemente dall'illecito che eventuali comportamenti possano determinare.

Il presente sistema disciplinare viene costantemente monitorato dall'OdV e dalla Direzione Risorse Umane.

4.2 Sanzioni e misure nei confronti dei dipendenti

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

Con riferimento alle sanzioni irrogabili nei riguardi di detti lavoratori dipendenti, nel rispetto delle procedure di cui all'art. 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori), esse rientrano tra quelle previste dal Contratto Collettivo Nazionale dei Lavoratori Metalmeccanici.

In particolare, in applicazione dei criteri di correlazione tra le mancanze dei lavoratori ed i provvedimenti disciplinari contenuti nel vigente Contratto Collettivo, si prevede che:

a) incorre nei provvedimenti di AMMONIZIONE SCRITTA, MULTA, SOSPENSIONE il lavoratore che violi le procedure interne previste dal Modello (ad es. che non osservi le procedure prescritte, ometta di dare comunicazione all’OdV delle informazioni prescritte, ometta di svolgere controlli, ecc.) o adotti, nell’espletamento delle attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una *“mancanza che porti pregiudizio alla disciplina, alla morale, all’igiene ed alla sicurezza dello stabilimento”* di cui al CCNL.

incorre nel provvedimento di LICENZIAMENTO CON PREAVVISO il lavoratore che adotti nell’espletamento delle attività nelle aree a rischio un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, dovendosi ravvisare in tale comportamento un atto tale da far venir meno radicalmente la fiducia dell’azienda nei confronti del lavoratore ovvero qualora al lavoratore siano comminati due provvedimenti di sospensione in un arco temporale di 24 mesi.

b) incorre, infine, nel provvedimento di LICENZIAMENTO SENZA PREAVVISO il lavoratore che adotti, nell’espletamento delle attività nelle aree a rischio un comportamento palesemente in violazione delle prescrizioni del Modello, tale da determinare la concreta applicazione a carico della società di misure previste dal Decreto, dovendosi ravvisare nel suddetto comportamento una condotta tale da provocare *“alla società grave nocumento morale e/o materiale”*, nonché da costituire *“delitto a termine di legge”* di cui al CCNL.

Il tipo e l'entità di ciascuna sanzione saranno applicate in relazione:

- a) all'intenzionalità del comportamento o grado di negligenza, imprudenza, od imperizia con riguardo anche alla prevedibilità dell'evento;
- b) al comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- c) alle mansioni del lavoratore;
- d) alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- e) alle altre particolari circostanze che accompagnano la violazione.

4.3 Sanzioni e misure nei confronti dei dirigenti

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

4.4 Misure nei confronti di amministratori e sindaci

Nel caso di violazione del Modello da parte degli amministratori o dei Sindaci di ADP Dealer Services Italia S.r.l., L'OdV ne informerà il Consiglio di Amministrazione ed il Collegio Sindacale, i quali daranno informazione alla società controllante e procederanno alla convocazione dell'Assemblea dei Soci per deliberare in merito alla assunzione delle opportune iniziative previste dalla normativa e, se necessario, alla revoca del mandato.

4.5 Misure nei confronti di collaboratori esterni e partner

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, grazie all'attivazione di opportune clausole, la risoluzione del rapporto contrattuale. L'OdV, con l'opportuno supporto legale, cura l'elaborazione, l'aggiornamento e l'inserimento nelle lettere d'incarico o negli accordi di collaborazione di tali specifiche clausole contrattuali che prevedranno anche l'eventuale richiesta di risarcimento dei danni derivanti alla società dall'applicazione da parte del giudice delle misure previste dal Decreto.

5. Modello e Codice Etico

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice etico (allegato sub.4), pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto e nel TUF, una portata diversa rispetto al Codice stesso.

Sotto tale profilo, infatti:

- il Codice etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte della Società allo scopo di esprimere dei principi di “deontologia aziendale” che ADP Dealer Services Italia s.r.l. riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti;
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto e nel TUF, finalizzate a prevenire la commissione dei Reati e degli illeciti (per fatti che, commessi apparentemente nell'interesse o a vantaggio dell'Azienda, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

6. Il Modello organizzativo di ADP Dealer Services Italia s.r.l.: costruzione, principi e struttura

In ossequio alla previsione normativa ed a quanto previsto dalle Linee Guida di Confindustria, per la redazione del presente Modello Organizzativo si è previamente provveduto alla mappatura dei rischi aziendali.

In particolare la dirigenza aziendale è stata resa edotta delle previsioni normative introdotte dal Decreto 231/01 e, al fine di costruire un Modello Organizzativo idoneo a prevenire i reati sia dolosi che colposi previsti dal Decreto, si è provveduto ad individuare la struttura organizzativa della società, l'articolazione territoriale, l'organigramma, le procedure decisionali, quelle per la redazione del bilancio e quelle di reporting.

Si descrivono brevemente le fasi in cui si è articolato il lavoro di individuazione delle aree di rischio:

1. **“As-is analysis”**. Le attività sensibili sono state individuate attraverso l'esame della documentazione aziendale (ultimo bilancio di esercizio, verbale del consiglio di amministrazione e dell'assemblea dei soci, documento sulla sicurezza, procedure aziendali, procure ecc.) e la sottoposizione dell'intero Management Team ad appositi questionari che sono stati sottoscritti e verranno messi a disposizione e conservati dall'OdV.

In particolare sono stati intervistati i seguenti responsabili aziendali nelle rispettive funzioni come rilevate al settembre 2008):

Amministratore Delegato: Giovanni De Meis

General Manager: Alberto Toniolo

Internal Information System (IIS) & Health/Safety manager: Roberto Galione

F & A Director: Pier Giovanni Fabbri Colabich

HR Director: Luca Bauckneht

Marketing Manager: Alessandra Penada

Support Director: Luciano Legovich

R & D Director: Giorgio Lazzaro

Italy Service Director: Giuseppe Fasolino

Sales Director: Francesco Giglio

After Sales Director: Paolo Angeloni

Al fine di verificare l'attendibilità delle risposte fornite singolarmente dai componenti del Management Team il questionario è stato sottoposto ad alcuni dipendenti appartenenti alle diverse aree aziendali i quali, selezionati del tutto casualmente, hanno provveduto alla compilazione in forma totalmente anonima.

2. *“Gap analysis”*

Come già più sopra anticipato, la società ADP Dealer Services Italia s.r.l si è già dotata di un articolato sistema di procedure; sulla base della situazione attuale e delle previsioni del Decreto 231/01, si sono individuate le azioni di miglioramento delle attuali procedure interne e dei requisiti organizzativi essenziali per la definizione del Modello organizzativo.

Nella predisposizione del presente Modello si è dunque tenuto conto dei principi, delle procedure e dei sistemi di controllo esistenti e già operanti nella società in quanto idonei a valere anche come misure di prevenzione dei reati e degli illeciti previsti dal Decreto.

In particolare quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali ed effettuare i controlli sull'attività d'impresa, soprattutto in relazione ai reati ed agli illeciti da prevenire, ADP Dealer Services Italia s.r.l ha individuato:

- il Codice Etico adottato dalla società;
- il sistema sanzionatorio di cui al CCNL applicabile;
- il documento sulla sicurezza ex D.L.vo 81/08.

Le regole, le procedure e i principi di cui agli strumenti elencati, sebbene non espressamente riportati nel presente Modello, fanno comunque parte del sistema di organizzazione e controllo che lo stesso intende integrare e che tutti i destinatari dello stesso, in relazione al tipo di rapporto in essere con la società, sono tenuti a rispettare.

A seguito dell'analisi del contesto aziendale e della mappatura dei rischi brevemente descritta, è emerso che le attività sensibili riguardano:

- a) i reati societari (parte speciale 1)
- b) i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (parte speciale 2)
- c) i reati informatici (parte speciale 3)
- d) i reati contro la Pubblica Amministrazione (parte speciale 4)
- e) i reati ambientali (parte speciale 5)

7. Formazione e diffusione del Modello

7.1 Formazione ed informazione dei Dipendenti

Ai fini dell'efficacia del presente Modello, è obiettivo di ADP Dealer Services Italia s.r.l. garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti dei Dipendenti, sia già presenti in azienda sia da inserire in futuro. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in

relazione al diverso livello di coinvolgimento delle risorse medesime nelle Attività Sensibili.

La comunicazione iniziale

L'adozione del presente Modello è comunicata ai Dipendenti al momento dell'adozione stessa.

Ai nuovi assunti viene consegnato un set informativo, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza. Tale set informativo dovrà contenere, oltre ai documenti di regola consegnati al neo-assunto, utenze informatiche e credenziali per accedere alla Intranet intesa come repository ufficiale del Modello Organizzativo, del Documento di valutazione dei rischi ex art. 17 D.Lgs. 81/08, del testo aggiornato del D.Lgs. 231/2001. Inoltre verrà fornita copia cartacea del Codice Etico. Tali soggetti saranno tenuti a rilasciare ad ADP Dealer Services Italia s.r.l una dichiarazione sottoscritta ove si attesti la ricezione del set informativo nonché la integrale conoscenza dei documenti allegati e l'impegno ad osservarne le prescrizioni.

La formazione

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'aver o meno funzioni di rappresentanza della società.

In particolare, saranno previsti livelli diversi di informazione e formazione attraverso idonei strumenti di diffusione per:

1. dipendenti che rivestono la qualifica di dirigenti;
2. dipendenti che non rivestono la qualifica di dirigenti.

Tutti i programmi di formazione avranno un contenuto minimo comune consistente nell'illustrazione dei principi del D.Lgs. 231/01, degli elementi costitutivi il Modello di Organizzazione Gestione e Controllo, delle singole fattispecie di reato previste dal D.Lgs. 231/01 e dei comportamenti considerati sensibili in relazione al compimento dei sopraccitati reati.

In aggiunta a questa matrice comune ogni programma di formazione sarà modulato al fine di fornire ai suoi fruitori gli strumenti necessari per il pieno rispetto del dettato del Decreto in relazione all'ambito di operatività e alle mansioni dei soggetti destinatari del programma stesso.

La partecipazione ai programmi di formazione sopra descritti è obbligatoria e il controllo circa l'effettiva frequenza è demandata all'OdV.

All'OdV è demandato altresì il controllo circa la qualità dei contenuti dei programmi di formazione così come sopra descritti.

7.2 Informazione dei consulenti e dei collaboratori esterni

Relativamente ai consulenti ed ai collaboratori esterni, sono istituiti appositi sistemi di informativa nei loro confronti.

PARTE SPECIALE 1

I reati societari (D.L.vo 231/2001 - Art. 24 bis) e il riciclaggio (D.L.vo 231/2001 - Art. 25 octies)

1. FALSITÀ IN COMUNICAZIONI, PROSPETTI E RELAZIONI

- *False comunicazioni sociali (art. 2621 cod. civ.)*
- *False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 cod. civ.)*

L'ipotesi di reato di cui all'art. 2621 cod. civ. si configura nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, nell'intento di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto espongano, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero omettano informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione.

L'ipotesi di reato di cui all'art. 2622 cod. civ. si configura nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, nell'intento di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, espongano nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero

omettano informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionando un danno patrimoniale alla società, ai soci o ai creditori.

Le due ipotesi di reato, di cui agli articoli 2621 e 2622 cod. civ., prevedono una condotta che coincide quasi totalmente e si differenziano solo per il verificarsi (art. 2622 cod. civ.) o meno (art. 2621 cod. civ.) di un danno patrimoniale alla società, ai soci o ai creditori.

In entrambi i casi la punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscano in misura non superiore al 10 per cento da quella corretta.

Si precisa che:

- le informazioni false od omesse devono essere tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- la responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

In entrambi i casi i soggetti attivi dei reati sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori.

- *Falso in prospetto (art. 173-bis TUF)*

Tale ipotesi di reato consiste nell'esporre false informazioni ovvero nell'occultare dati o notizie all'interno dei prospetti (per tali intendendosi i documenti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio) secondo modalità idonee ad indurre in errore i destinatari dei prospetti stessi.

Si precisa che:

- deve sussistere l'intenzione di ingannare i destinatari dei prospetti;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.

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

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

- *Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 174-bis TUF)*

L'ipotesi di reato di cui all'art. 2624 cod. civ. consiste in false attestazioni od occultamento di informazioni, nelle relazioni o in altre comunicazioni della società di revisione, concernenti la situazione economica, patrimoniale o finanziaria della società

sottoposta a revisione, secondo modalità idonee ad indurre in errore i destinatari delle comunicazioni stesse.

Si precisa che:

- deve sussistere la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- il reato in questione viene configurato come delitto ovvero come contravvenzione a seconda che abbia cagionato o meno ai destinatari delle comunicazioni un danno patrimoniale.

L'ipotesi di reato di cui all'art. 174-bis TUF è stata introdotta dalla legge 28 dicembre 2005, n. 262 (*“Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari”*) ed è applicabile specificamente ai responsabili della revisione delle società con azioni quotate, delle società da queste controllate e delle società che emettono strumenti finanziari diffusi fra il pubblico in misura rilevante ai sensi dell'art. 116 TUF. Il reato in esame si differenzia dall'ipotesi di cui all'art. 2624 cod. civ. anche in quanto non è richiesta la consapevolezza della falsità in capo all'autore della condotta delittuosa.

Sia per l'art. 2624 cod. civ. che per l'art. 174-bis TUF, soggetti attivi dei rispettivi reati sono i responsabili della società di revisione. Sennonché, in entrambi i casi, potrebbero essere coinvolti, a titolo di concorso nel reato, anche i componenti degli organi di amministrazione e di controllo del Gruppo e i suoi dipendenti. È, infatti, ipotizzabile il concorso eventuale, ai sensi dell'art. 110 cod. pen., degli amministratori, dei sindaci, o di altri soggetti della società sottoposta a revisione, che abbiano determinato o istigato la condotta illecita del responsabile della società di revisione.

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

2. TUTELA PENALE DEL CAPITALE SOCIALE

- *Indebita restituzione dei conferimenti (art. 2626 cod. civ.)*

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

Soggetti attivi del reato possono essere solo gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 cod. pen., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

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

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite.

Si fa presente che:

- la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 cod. pen., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

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

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

Si fa presente che:

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

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

- *Operazioni in pregiudizio dei creditori (art. 2629 cod. civ.)*

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

- *Formazione fittizia del capitale (art. 2632 cod. civ.)*

Tale ipotesi di reato è integrata dalle seguenti condotte:

- a) formazione o aumento in modo fittizio del capitale sociale, anche in parte, mediante attribuzione 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, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori ed i soci conferenti.

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

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

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono esclusivamente i liquidatori.

3. TUTELA PENALE DEL REGOLARE FUNZIONAMENTO DELLA SOCIETÀ

- *Impedito controllo (art. 2625 cod. civ.)*

Tale ipotesi di reato consiste nell'impedire od ostacolare, mediante occultamento di documenti o con altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione.

Per tali ipotesi è prevista una sanzione amministrativa pecuniaria.

Le sanzioni sono maggiorate qualora tale condotta abbia cagionato un danno ai soci.

L'illecito può essere commesso esclusivamente dagli amministratori.

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

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

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

4. TUTELA PENALE CONTRO LE FRODI

- *Aggiotaggio (art. 2637 cod. civ.)*

Tale ipotesi di reato consiste nel diffondere notizie false ovvero nel realizzare operazioni simulate o altri artifici, concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero nell'incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Anche questo è un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

5. TUTELA PENALE DELLE FUNZIONI DI VIGILANZA

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

Si tratta di un'ipotesi di reato che può essere realizzato con due condotte distinte:

- la prima si realizza (i) attraverso l'esposizione nelle comunicazioni previste dalla legge alle Autorità pubbliche di Vigilanza (al fine di ostacolare l'esercizio delle funzioni di queste ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero (ii) mediante l'occultamento, con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria.

La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;

- la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche Autorità, attuato consapevolmente ed in qualsiasi forma, anche omettendo le comunicazioni dovute alle Autorità medesime.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori.

RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA (D.L.vo 231/2001 - Art. 25 octies)

Ricettazione (648 c.p.)

Fuori dei casi di concorso nel reato, chi, al fine di procurare a sè o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da 516 euro a 10.329 euro.

La pena è della reclusione sino a sei anni e della multa sino a 516 euro, se il fatto è di particolare tenuità.

Le disposizioni di questo articolo si applicano anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

Riciclaggio (648 bis c.p.)

Fuori dei casi di concorso nel reato, chiunque 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, è

punito con la reclusione da quattro a dodici anni e con la multa da € 1.032,00 a € 15.493,00.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La pena è diminuita se il denaro, i beni o le altre utilità provengano da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

Si applica l'ultimo comma dell'articolo 648.

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

Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da € 1.032,00 a € 15.493,00.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648.

Si applica l'ultimo comma dell'articolo 648.

Aree a rischio e Gap Analysis

In ordine ai suddetti reati societari e di riciclaggio e ricettazione, risulta a rischio l'intera area di Amministrazione e Finanza - il cui responsabile di funzione è il Dott. Pier Giovanni Fabbri Colabich - il Consiglio di Amministrazione e i Consulenti esterni addetti alla redazione del Bilancio.

La società ADP Dealer Services Italia s.r.l è dotata di un sistema informatico, che deve essere necessariamente attivato per qualsivoglia operazione di carattere contabile, che registra automaticamente tutte le operazioni in entrata ed in uscita. La registrazione di tutta la contabilità ordinaria della società avviene attraverso “UNITE” che è un sistema gestionale, collocato in Inghilterra, sviluppato su software Navision.

La società ADP Dealer Services Italia S.r.l. è inoltre tenuta a riportare mensilmente all’Head Quarter di Automatic Data Processing Inc., alla cui direzione e coordinamento è assoggettata ex art. 2497 bis c.c., il risultato economico parziale che pertanto viene costantemente controllato dall’Head Quarter della suddetta società. Il programma utilizzato per la gestione della reportistica è “HYPERION”.

Il report mensile è composto da una serie di tabelle standard in cui vengono riportate tutte le statistiche richieste da Headquarters, sia consuntive che previsionali (Budget annuale e Forecast): le principali sono PL (conto economico), BS (stato patrimoniale), K-Stats (ordini pervenuti nel periodo, ordini installati nel periodo, portafoglio ordini), Ageing (stato dei crediti), Headcount (conta del personale e distribuzione nei reparti), Other Keystats (altre statistiche in particolare confronto canoni clienti persi - nuovi clienti acquisiti).

Il bilancio di ADP Dealer Services Italia S.r.l., sebbene non richiesto dalla Legge, viene certificato da una società di revisione (Deloitte & Touche LLP).

Dall’analisi dei rischi relativi ai reati societari ed al riciclaggio, tenuto conto delle procedure aziendali già in essere (Procedure Acquisti, Emissione Accrediti, Gestione Crediti, Procedura Investimenti, Procedura di tenuta della Cassa, ecc.) che qui si richiamano integralmente come parte integrante del presente Modello Organizzativo, nonché del fatto che il bilancio è certificato, emerge che il rischio della commissione dei suddetti reati risulta essere basso. Inoltre, su richiesta di ADP Inc., i processi di ciclo

attivo, ciclo passivo, elaborazione paghe e in generale tutti i processi aventi ad oggetto trasferimenti di denaro, sono conformi a ulteriori e severe procedure di controllo che ottemperano al Sarbanes-Oxley Act (SOX), legge federale americana emanata nel 2002 finalizzata a garantire la trasparenza delle scritture contabili e a migliorare la Corporate Governance.

Principi generali

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali di ADP Dealer Services Italia s.r.l e dei Dipendenti e Consulenti che hanno responsabilità nella redazione del bilancio di 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 *ter* del D.Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente parte speciale.

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
2. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;

3. assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

4. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

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

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;

b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società.

Contratti

Nei contratti con i consulenti e con i collaboratori esterni deve essere contenuta apposita clausola che regoli le conseguenze da parte degli stessi all'infrazione delle norme di cui al Decreto 231/01 nonché del presente Modello.

I controlli dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività sociali potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere.

Il responsabile del settore amministrazione e finanza è tenuto a trasmettere all'OdV una relazione circa le operazioni di natura straordinaria e non ricorrente: tale relazione deve essere sufficientemente documentata e idonea a giustificare l'operazione illustrandone l'intera procedura.

PARTE SPECIALE 2

I reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies)

L'art. 25-*septies* fa riferimento ai reati di cui agli artt. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. Tali fattispecie delittuose riguardano unicamente le ipotesi in cui l'evento sia stato determinato da “colpa specifica” che richiede che l'evento si verifichi a causa della inosservanza delle norme per la prevenzione degli infortuni sul lavoro.

- Omicidio colposo (art. 589 cod. pen.)

Il reato si configura ogni qualvolta un soggetto cagioni per colpa la morte di altro soggetto.

- Lesioni personali colpose gravi o gravissime (art. 590 comma 3 cod. pen.)

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni ad altro soggetto lesioni gravi o gravissime.

Ai sensi del comma 1 dell'art. 583 cod. pen., la lesione è considerata grave nei seguenti casi:

“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”.

Ai sensi del comma 2 dell'art. 583 cod. pen., la lesione è considerata invece gravissima se dal fatto deriva:

“una malattia certamente o probabilmente insanabile;

la perdita di un senso;

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;

la deformazione, ovvero lo sfregio permanente del viso”.

Perché si venga a configurare la responsabilità amministrativa della Società ai sensi del Decreto, l'art. 5 del Decreto medesimo esige però che i reati siano stati commessi nel suo interesse o a suo "vantaggio" (ad esempio in termini di risparmi di costi o di tempi).

Proprio in relazione a tali reati, secondo quanto previsto ai sensi dell'art. 30 D.L.vo 81/08, il modello di organizzazione e di gestione *“deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:*

a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

- b) *alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;*
- c) *alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;*
- d) *alle attività di sorveglianza sanitaria;*
- e) *alle attività di informazione e formazione dei lavoratori;*
- f) *alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;*
- g) *alla acquisizione di documentazioni e certificazioni obbligatorie di legge;*
- h) *alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.*

Il modello organizzativo e gestionale di cui al comma 1 [del medesimo art. 30 n.d.r.] deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività' in relazione al progresso scientifico e tecnologico.”.

Mappatura delle aree a rischio e gap analysis

In relazione ai reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme di tutela della salute e sicurezza sul lavoro, non è possibile escludere aprioristicamente alcun ambito di attività, dal momento che tale casistica di reati può di fatto investire la totalità delle componenti aziendali.

Nel caso specifico di ADP Dealer Services Italia s.r.l, la società ha proceduto a redigere il Documento della Sicurezza previsto dagli artt. 17 e 28 del D. Lgs. 9 aprile 2008, n. 81, il quale prevede specifiche ed adeguate procedure di prevenzione dei rischi (Sistema di gestione della salute e sicurezza del lavoro) in relazione ai reati summenzionati che si allega sub 4) e che si richiama quale parte integrante del presente Modello.

Come si evince da tale documento, la valutazione del rischio potenziale d'infortunio è stata valutata con riferimento alle diverse aree aziendali ma, considerata l'attività svolta dalla società, le pregnanti procedure di prevenzione e misure di sicurezza già poste in essere dalla società e il fatto che negli ultimi 20 anni non si sono verificati incidenti di rilievo, il rischio di infortuni è da considerarsi globalmente basso.

Si ritiene in ogni caso di integrare le procedure aziendali già esistenti al fine di coordinarle con la disciplina del D. Lgs 231/01, dando adempimento al disposto dell'art. 30 D. Lgs. 81/2008.

Inoltre è stata prevista una specifica procedura, alle pagine 73 e ss. del presente Modello, relativa alla prevenzione dell'infortunistica stradale che, per quanto riferito dai dirigenti aziendali (confermato dai questionari anonimi) e da quanto risulta dal registro infortuni, risulta essere "l'ambito lavorativo" con maggiori rischi.

Definizioni

Ambiente di lavoro: tutti i locali di pertinenza di ADP Dealer Services Italia S.r.l. frequentati dai lavoratori.

ASPP o Addetti al Servizio di Prevenzione e Protezione: i soggetti designati per l'espletamento dei compiti rientranti nel Servizio di Prevenzione e Protezione.

Decreto 81/2008: Decreto legislativo del 9 aprile 2008 n. 81 (Testo Unico Sicurezza e Salute sui luoghi di Lavoro).

Datore di Lavoro: il soggetto titolare del rapporto di lavoro o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa ovvero dell'unità produttiva in quanto titolare dei poteri decisionali e di spesa.

Decreto 626: Decreto legislativo del 19 settembre 1994 n. 626 e successive modifiche ed integrazioni sul miglioramento della sicurezza e della salute dei lavoratori durante il lavoro.

Dirigente: il soggetto cui il Datore di Lavoro abbia delegato, in ragione della specificità e complessità della propria entità organizzativa, compiti e responsabilità in tema di sicurezza e salute sui luoghi di lavoro.

DVR o Documento di Valutazione dei Rischi: il documento redatto dal Datore di Lavoro ai sensi degli artt. 17, 18, 28 e 29 del D. Lgs. 9 aprile 2008, n. 81 contenente una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, l'individuazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuale conseguente a tale valutazione ed il programma.

Medico Competente: il medico preposto all'attività di Sorveglianza Sanitaria.

Preposto: la persona che, in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori esercitando un funzionale potere di iniziativa.

Reati commessi in violazione delle norme antinfortunistiche: i reati di cui all'art. 25-septies del D. Lgs. 231/2001, ovvero l'omicidio colposo (art. 589 cod. pen) e le lesioni personali colpose gravi o gravissime (art. 590 terzo comma cod. pen.) commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

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

RSPP o Responsabile del Servizio di Prevenzione e Protezione: il soggetto responsabile del Servizio di Prevenzione e Protezione nominato dal Datore di Lavoro.

Sorveglianza Sanitaria: l'insieme degli accertamenti, preventivi e periodici, effettuati dal Medico Competente nei casi previsti dalla normativa, in relazione alla valutazione dei rischi, finalizzati a valutare l'idoneità del lavoratore alla mansione specifica.

SGSL o Sistema di gestione della salute e della sicurezza sul lavoro: si tratta di una procedura, contenuta in apposita sezione del “Documento di valutazione dei rischi” (pagg. 49 e ss.) che definisce le modalità per individuare all’interno della struttura organizzativa aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della politica aziendale di prevenzione, nel rispetto delle norme di salute e sicurezza vigenti.

Figure rilevanti: competenze, compiti e doveri

Il datore di lavoro

Al Datore di Lavoro sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti compiti non delegabili:

- 1) valutare tutti i rischi per la sicurezza e per la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, anche nella scelta delle attrezzature di lavoro e delle sostanze o dei preparati chimici impiegati, nonché nella sistemazione dei luoghi di lavoro;
- 2) elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi (da custodirsi presso l'azienda) nonché il SGSL, contenenti:
 - una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella quale sono specificati i criteri adottati per la valutazione stessa;
 - l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione dei rischi;
 - il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il RSPP e con il Medico Competente nei casi in cui sia obbligatoria la

Sorveglianza Sanitaria. La valutazione dei rischi è oggetto di consultazione preventiva con il Rappresentante dei Lavoratori per la Sicurezza, e va nuovamente effettuata in occasione di modifiche del processo produttivo significative ai fini della sicurezza e della salute dei lavoratori;

3) designare il Responsabile del Servizio di Prevenzione e Protezione interno o esterno all'azienda.

Al Datore di Lavoro sono attribuiti i seguenti altri compiti dallo stesso delegabili a soggetti qualificati, che riguardano, tra l'altro, il potere di: a) indire almeno una volta all'anno la "riunione periodica di prevenzione e protezione dai rischi" ove partecipano, oltre al Datore di Lavoro medesimo o a un suo rappresentante, il RSPP, il Medico Competente e il Rappresentante dei Lavoratori per la Sicurezza; b) nominare il Medico Competente e gli eventuali ASPP; c) designare i lavoratori incaricati dell'attuazione delle misure di emergenza e pronto soccorso; d) fornire ai lavoratori i necessari ed idonei dispositivi di protezione individuale e aggiornare le misure di prevenzione; e) richiedere l'osservanza da parte dei lavoratori delle norme vigenti e delle disposizioni aziendali in materia di sicurezza ed igiene del lavoro; f) richiedere l'osservanza da parte del Medico Competente degli obblighi previsti dalla legge; g) adottare le misure di protezione per il rischio grave e immediato; h) istituire ed aggiornare il registro infortuni; i) consultare le rappresentanze dei lavoratori per la sicurezza.

In base al CCNL è attribuito inoltre al Datore di Lavoro, o ad un Dirigente da questi delegato, il compito di adottare provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservano le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o altrui sicurezza.

Il preposto

I principali doveri del preposto, secondo le proprie attribuzioni e poteri, sono:

- a) sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di persistenza dell'inosservanza, informare i loro superiori diretti;
- b) verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
- c) richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- d) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- e) astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;
- f) segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;
- g) frequentare appositi corsi di formazione secondo quanto previsto dall'art. 37 D.L.vo 81/08.

Il Responsabile del Servizio di Prevenzione e Protezione (RSPP)

La società ADP Dealer Services Italia s.r.l ha nominato quale proprio RSPP, l'Internal Information System (di seguito IIS) & Health/Safety Manager, che è in possesso del titolo di istruzione richiesto dalla normativa vigente e che ha frequentato e frequenta corsi di formazione e di aggiornamento.

Il Responsabile dei Servizi di Prevenzione e Protezione, il quale deve essere considerato quale il responsabile delle procedure aziendali in materia, svolgerà un controllo tecnico - operativo di primo grado - conformemente a quanto disposto dalle Linee Guida UNI – INAIL per un sistema di gestione della salute e sicurezza del lavoro (SGSL), nonché dalle Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/01 emanate da Confindustria ed infine dall'art. 30 del D.Lgs. 08 -volto alla verifica del raggiungimento degli obiettivi di sicurezza pianificati, conformemente a quanto disposto alle pp. 56 e 78 del “Documento di valutazione dei rischi”, con l'ausilio delle altre risorse interne della struttura aziendale, come meglio individuate nel Documento di valutazione dei rischi - SGSL, alle pp. 80 e ss. ed anche di un Consulente esterno, il quale riveste anche il ruolo di Medico competente, che ha partecipato alla redazione del Documento della Sicurezza ai sensi degli artt. 17 e 28 del D. Lgs. 9 aprile 2008, n. 81.

Più specificamente il RSPP :

- ha provveduto ad individuare i fattori di rischio, valutare i rischi e individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente e sulla base della specifica conoscenza dell'organizzazione aziendale;

- ha provveduto a collaborare con il Datore di Lavoro e con il Medico Competente, nei casi in cui sia obbligatoria la sorveglianza sanitaria, all'elaborazione del Documento di Valutazione dei Rischi;
- ha provveduto e deve provvedere costantemente a collaborare all'elaborazione delle misure preventive e protettive e dei sistemi di controllo di tali misure;
- ha provveduto e deve provvedere costantemente ad elaborare procedure di sicurezza per le varie attività aziendali;
- deve provvedere costantemente a controllare l'efficienza delle misure preventive e protettive anche in rapporto agli aggiornamenti tecnologici ed alle "buone prassi" del settore;
- deve continuamente monitorare gli ambienti di lavoro, mantenendosi in stretto contatto con il Rappresentante dei Lavoratori per la Sicurezza, al fine di cogliere eventuali rischi residuali segnalandoli all'OdV ed al Consiglio di Amministrazione;
- deve provvedere a proporre programmi di informazione e formazione dei lavoratori;
- deve partecipare alla "riunione periodica di prevenzione e protezione dai rischi";
- deve partecipare alle consultazioni in materia di tutela della salute e della sicurezza;
- deve informare i lavoratori, a nome e per conto del Datore di Lavoro, sui rischi, sulle misure di prevenzione e protezione, sulle procedure e sui nominativi dei lavoratori incaricati delle misure di emergenza e di pronto soccorso, nonché, ove previsto, del medico competente;

Per espletare i compiti assegnati, il RSPP è adeguatamente informato dal Datore di Lavoro in merito a:

- la natura dei rischi;

- l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
- la descrizione degli impianti e dei processi produttivi;
- i dati del registro degli infortuni e delle malattie professionali;
- le prescrizioni degli organi di vigilanza.

L'eventuale sostituzione del RSPP deve essere comunicata all'OdV con l'espressa indicazione delle motivazioni a supporto di tale decisione.

L'Organismo di Vigilanza

L'OdV nell'esercizio delle sue prerogative e funzioni, come più sopra esposte, eserciterà un controllo sulla funzionalità del sistema (controllo di secondo grado), come meglio specificato nel Documento di valutazione dei rischi - SGSL alle pp. 81 e ss., allo scopo di stabilire se il sistema di gestione della salute e sicurezza sul lavoro, è conforme a quanto pianificato, è correttamente applicato, mantenuto attivo e consente di raggiungere gli obiettivi. Il monitoraggio di funzionalità del sistema dovrebbe consentire al vertice aziendale l'adozione delle decisioni strategiche di propria competenza, quali ad esempio l'adeguamento della politica aziendale.

Più specificamente l'OdV dovrà:

1. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati commessi in violazione delle norme antinfortunistiche. Con riferimento a tale punto l'OdV - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia in possesso di requisiti formativi e professionali pari a quelli del RSPP che assicurino l'obiettività e l'imparzialità, nonché l'indipendenza dal settore di lavoro

sottoposto a verifica ispettiva - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato e proporrà ai soggetti competenti della Società eventuali azioni migliorative;

2. proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

3. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;

Allo scopo di svolgere i propri compiti, l'OdV può:

a) partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;

b) accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

Il Medico Competente

La società ADP Dealer Services Italia s.r.l ha nominato il proprio Medico del Lavoro che è in possesso del titolo richiesto dalla normativa vigente.

Il Medico Competente deve provvede a:

- collaborare con il Datore di Lavoro e con il Responsabile del Servizio di Prevenzione e Protezione alla predisposizione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori;

- effettuare le visite mediche preventive e periodiche previste dalla legge e da programmi di prevenzione opportunamente stabiliti;
- fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informarli sui risultati;
- istituire ed aggiornare, per ogni lavoratore sottoposto a Sorveglianza Sanitaria, le cartelle sanitarie e di rischio, con salvaguardia del segreto professionale;
- visitare gli ambienti di lavoro, congiuntamente al RSPP, redigendo specifico verbale, con la frequenza prestabilita in relazione alle caratteristiche dell'Unità produttiva;
- comunicare, in occasione della riunione periodica di prevenzione e protezione dai rischi, i risultati anonimi collettivi degli accertamenti sanitari, fornendo le informazioni necessarie;
- collaborare con il Datore di Lavoro alla predisposizione del servizio di pronto

Il Rappresentante dei Lavoratori per la Sicurezza

La società ADP Dealer Services Italia s.r.l ha designato, in conformità a quanto previsto dagli accordi sindacali in materia, il proprio RLS in rappresentanza dei lavoratori.

Il RLS:

- accede ai luoghi di lavoro;
- è consultato preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- è consultato sulla designazione del RSPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso;
- è consultato in merito all'organizzazione delle attività formative;

- promuove l'elaborazione, l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei lavoratori;
- partecipa alla "riunione periodica di prevenzione e protezione dai rischi";
- riceve informazioni inerenti la valutazione dei rischi e le misure di prevenzione relative e, ove ne faccia richiesta e per l'espletamento della sua funzione, copia del Documento di Valutazione dei Rischi e del registro infortuni.

I lavoratori

È cura di ciascun lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite.

I lavoratori devono:

- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze e i preparati pericolosi, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
- segnalare immediatamente al Datore di Lavoro, al dirigente o al preposto le deficienze dei mezzi e dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al rappresentante dei lavoratori per la sicurezza;

- non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni né manovre che non siano di loro competenza ovvero che possano compromettere la sicurezza propria o di altri lavoratori;
- sottoporsi ai controlli sanitari previsti nei loro confronti;
- contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

Procedure aziendali

La Società ADP Dealer Services Italia s.r.l ha elaborato ed approvato il Documento di Valutazione dei Rischi e di predisposizione delle misure di prevenzione e protezione conseguenti (all. sub 5) da custodirsi presso l'azienda, contenente, ai sensi degli artt. 17, 18 e 28 del D.L.vo 81/08:

- a) una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
- b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);
- c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
- d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;

f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

La Società ADP Dealer Services Italia s.r.l, inoltre, ha predisposto una procedura interna per la sicurezza e per la gestione delle emergenze (incendio - evacuazione - malore) denominata Procedura Emergenze - versione 3/07 - che si intende integralmente richiamata, così come la Procedura Sicurezza sempre versione 3/07.

La società ha il compito di adottare provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservano le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o altrui sicurezza.

Informazione e formazione

Come già previsto nella parte generale, la Società è tenuta a fornire adeguata informazione ai dipendenti e nuovi assunti circa i rischi specifici dell'impresa, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate nonché sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del D.Lgs. 231/2001 nonché del D Lgs. 123/07.

A tal fine:

- deve essere documentata/diffusa l'informativa sulla gestione delle emergenze (incendio - evacuazione - malore)

- i dipendenti e nuovi assunti devono ricevere informazione sulla nomina del RSPP e sul sistema organizzato per la gestione delle emergenze;
- deve essere fornita informazione e istruzione sull'uso delle attrezzature di lavoro messe a disposizione dei dipendenti;
- il RSPP e il Medico Competente devono essere coinvolti nella definizione delle informazioni;
- la Società deve fornire adeguata formazione a tutti i dipendenti in materia di sicurezza sul lavoro, come già specificamente previsto nel “Documento di valutazione dei rischi” alle pp. 66 e ss;
- il RSPP e il Medico Competente, ove presente, debbono partecipare alla stesura del piano di formazione;
- la formazione erogata deve prevedere questionari di valutazione dell'apprendimento;
- la Società deve effettuare periodiche esercitazioni di emergenza di cui deve essere data evidenza (attraverso, ad esempio, la verbalizzazione dell'avvenuta esercitazione con riferimento alle modalità di svolgimento e alle risultanze);
- di tutta l'attività di informazione e formazione sopra descritta deve essere data evidenza su base documentale, eventualmente anche mediante apposita verbalizzazione.
- tutta la documentazione relativa alle attività di informazione e formazione deve essere conservata a cura del RSPP e messa a disposizione dell'OdV;
- la Società è tenuta ad organizzare periodici incontri tra le funzioni preposte alla sicurezza sul lavoro fornendone comunicazione all'OdV.
-

Registri e documenti

Il registro infortuni deve essere sempre aggiornato e compilato in ogni sua parte e custodito presso la sede della società.

Nell'ipotesi di esposizione ad agenti cancerogeni o mutageni deve essere predisposto il registro degli esposti.

Deve essere data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente.

La Società deve tenere un archivio dei documenti che registrano gli adempimenti espletati in materia di sicurezza e igiene sul lavoro.

Costituiscono ulteriori documenti la cui istituzione è obbligatoria:

- il Documento di Valutazione dei Rischi e predisposizione delle misure di prevenzione e protezione conseguenti;
- il Piano di Sicurezza;
- il Piano di Emergenza;

L'OdV deve avere libero accesso in ogni momento a tutta la documentazione di cui sopra.

I lavori effettuati da imprese esterne e i contratti di appalto

Tutti i lavori effettuati da imprese esterne (lavori elettrici, di muratura ecc.) dovranno essere preceduti da un incontro tra i Responsabili dell'Ufficio acquisti e logistica e della sicurezza al fine di individuare tutte le azioni preventive da porre in atto per garantire la sicurezza del personale e la relativa informativa (a cura della Direzione Risorse Umane).

Nel corso di tale incontro verrà compilato il modulo di cui all'allegato 4 delle Procedure di Sicurezza che verrà archiviato dal Responsabile della Sicurezza.

Sarà cura dell'Ufficio Acquisti ottenere tutta la documentazione che i fornitori devono presentare relativamente alle proprie obbligazioni nell'esecuzione dei lavori secondo la normativa vigente (allegato 4 delle Procedure di Sicurezza) e, nel caso si tratti di opera soggetta al rilascio di certificato di conformità, il certificato stesso.

Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti di cui all'art. 7 del D.lgs 626/94 e dall'art. 10 del D.Lgs 271/99, tra i quali rientrano i doveri, in capo al Datore di Lavoro, di:

- verificare, anche attraverso l'iscrizione alla Camera di commercio, l'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare in appalto.
- fornire informazioni dettagliate agli appaltatori circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori;
- adottare misure volte a ridurre i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Il Datore di Lavoro committente, qualora siano presenti interferenze, elabora un unico Documento di Valutazione dei Rischi nel quale sono indicate le misure adottate per eliminare le interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera.

Nei contratti di somministrazione (art. 1559 c.c.), di appalto (art. 1655 c.c.) e di subappalto (art. 1656 c.c.), devono essere specificamente indicati i costi relativi alla sicurezza del lavoro. A tali dati possono accedere, su richiesta, il Rappresentante dei Lavoratori e le organizzazioni sindacali dei lavoratori.

Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

Progettisti, Fabbricanti, Fornitori e Installatori

I Progettisti dei luoghi, dei posti di lavoro e degli impianti sono tenuti al rispetto dei principi generali di prevenzione in materia di salute e sicurezza sul lavoro al momento delle scelte progettuali e tecniche e sono tenuti altresì a scegliere macchine nonché dispositivi di protezione rispondenti ai requisiti essenziali di sicurezza previsti nelle disposizioni legislative e regolamentari vigenti.

I Fabbricanti ed i Fornitori vendono, noleggiano e concedono in uso attrezzature, impianti e dispositivi di protezione individuale rispondenti alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro e di omologazione di prodotto.

Gli Installatori devono attenersi alle norme di sicurezza ed igiene del lavoro, nonché alle istruzioni fornite dai fabbricanti delle attrezzature

Contratti

Nei contratti con i Collaboratori esterni, i Consulenti esterni, con i Fornitori, con i Progettisti, i Fabbricanti e gli Installatori deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché del Modello.

Incidenti stradali

Relativamente agli incidenti stradali, che come si evince dal registro infortuni, nonché dal Documento di valutazione dei rischi ex D. Lgs. 81/2008, a pag. 44, sono di gran lunga la tipologia principale di infortunio, la società deve fornire ai dipendenti automobili aventi in dotazione tutte le misure di sicurezza richieste dalla legge, conformemente a quanto dispone l'art. 71 del D. Lgs. 81/98. In particolare tutti i modelli prevedranno la dotazione di airbag lato guidatore, fari fendinebbia, impianto di climatizzazione e soprattutto sistema di controllo della frenata ABS.

E' responsabilità del dipendente utilizzare l'autovettura assegnatagli dall'Azienda ovvero oggetto di noleggio secondo il criterio del buon padre di famiglia nel rispetto del Codice della Strada.

Nel caso in cui l'autovettura sia stata assegnata al lavoratore dall'Azienda secondo la "procedura Assegnazioni Beni Aziendali" e la "procedura trasferte" e relativi allegati il RSPP in collaborazione con l'Ufficio Risorse Umane si accerterà prima di procedere alla consegna dell'autovettura al lavoratore che questi sia in possesso di valida patente di guida.: sarà responsabilità del lavoratore provvedere alla manutenzione, di cui all'art. 70 comma 4 del D. Lgs. 81/08, del veicolo - a spese dell'Azienda - secondo le istruzioni del libretto uso e manutenzione, nonché secondo il criterio del buon padre di famiglia e nel rispetto del Codice della Strada.

L'assegnazione, l'uso e la restituzione della vettura dovrà avvenire secondo le modalità previste nella "procedura di sicurezza", "procedura Assegnazioni Beni Aziendali" e "procedura trasferte" e relativi allegati.

Come già previsto nella Procedura Sicurezza, eventuali incidenti stradali, sia durante l'orario lavorativo, sia in "itinere", ovvero nel tragitto casa/ufficio e viceversa, dovranno essere immediatamente comunicati, prima telefonicamente e poi per iscritto, alla Direzione Risorse Umane ed al Responsabile per la Sicurezza.

L'eventuale certificato medico dovrà pervenire, in originale o via fax, al più tardi il giorno successivo l'avvenuto incidente e dovrà essere redatto dalle Autorità Competenti, generalmente il pronto Soccorso (non da un medico generico), ed attestare come causa "infortunio sul lavoro".

Tutte le infrazioni al Codice della Strada che verranno contestate e dunque notificate alla società intestataria dei veicoli che fornisce ad ADP Dealer Services Italia s.r.l la "flotta aziendale", devono essere trasmesse a cura dell'Ufficio HR (Human Resources) al Responsabile del Servizio di Prevenzione e Protezione il quale dovrà tenere un apposito registro dei mezzi assegnati ad ogni dipendente con l'indicazione delle relative infrazioni contestate.

La società e l'OdV, che potrà consultare in ogni momento tale registro che dovrà comunque essergli trasmesso con scadenza annuale, potranno irrogare provvedimenti disciplinari nei confronti del lavoratore nei casi di gravi e reiterate violazioni del Codice della Strada ed in ogni caso qualora venga accertata dall'Autorità competente la guida in stato di alterazione da assunzione di sostanze stupefacenti ovvero la guida in stato di ebbrezza alcolica, laddove il tasso di alcool nel sangue sia superiore a 0,8 ml per litro, secondo quanto previsto dal vigente Contratto Collettivo e dal presente Modello.

Segnalazione mancato incidente

Come già previsto nella Procedura Emergenza, che si intende qui totalmente richiamata, al fine di mettere in atto tutte le precauzioni possibili per evitare incidenti o per prevenire

situazioni di pericolo, è stato predisposto apposito modulo (all. 10 alla predetta Procedura) per la segnalazione di eventi che avrebbero potuto generare incidenti o situazioni di pericoli per l'incolumità delle persone o per la sicurezza della sede: tale modulo, redatto da chi ha riscontrato il potenziale pericolo, deve essere inviato al Responsabile per la sicurezza, che, anche in tal caso, dovrà segnalare l'accaduto all'OdV per l'adozione degli opportuni accorgimenti.

Stress lavoro correlato

Nel corso del 2010 la Società ha provveduto - in ottemperanza all'integrazione del D.Lgs. 81/2008 attenente al rischio da stress lavoro correlato e relativi adempimenti in materia - a somministrare a tutti i dipendenti, sotto la supervisione metodologica di uno Psicologo del lavoro coordinato del Medico Competente, un questionario in forma anonima finalizzato alla valutazione della magnitudine del rischio in oggetto. L'analisi del questionario ha qualificato come "basso" il livello di rischio, non determinando quindi la necessità di implementare procedure *ad hoc*.

PARTE SPECIALE 3

I reati informatici (D.L.vo 231/2001 - Art. 24 bis)

Si descrivono brevemente qui di seguito le singole fattispecie dei reati informatici contemplati nel D.Lgs. 231/2001 all'art. 24 bis.

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

Tale ipotesi di reato si realizza con l'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escludere l'intruso.

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

Tale ipotesi di reato prevede due fattispecie: la prima è relativa alla fraudolenta intercettazione, impedimento ovvero interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi; la seconda si realizza, salvo che il fatto costituisca più grave reato, allorché si riveli in tutto o in parte, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle comunicazioni di cui alla precedente previsione normativa.

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

Tale ipotesi di reato colpisce chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

- *Danneggiamento di sistemi informatici e telematici (art. 635-bis c.p.)*

Tale ipotesi di reato prevede una sanzione per chiunque distrugga, deteriori o renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui.

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

Tale ipotesi di reato punisce chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

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

La norma in oggetto prevede una sanzione per chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.

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

Tale ipotesi di reato punisce le condotte di cui di cui all'articolo 635-quater che siano dirette a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento; il comma successivo prevede una pena ancora superiore qualora dal fatto derivi la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo sia reso, in tutto o in parte, inservibile.

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

Tale ipotesi prevede la punizione di chi, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

- *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 617-quinques c.p.)*

Tale ipotesi prevede la punizione di chi, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

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

Tale reato punisce il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

- *Documenti informatici (art. 491-bis c.p.)*

Tale ultima ipotesi estende la responsabilità penale per la falsità in atti a tutti i documenti informatici pubblici o privati aventi efficacia probatoria.

Aree a rischio

Dall'analisi dei rischi effettuata è emerso un rischio basso con riferimento alla commissione di tale tipologia di reati, in quanto non si sono mai verificati inconvenienti ed anche perché la società ha già adottato specifiche procedure che regolano l'utilizzo da parte dei dipendenti degli strumenti informatici e la protezione dei dati in essi contenuti. Si ritiene opportuno in ogni caso richiamare tali procedure direttamente nel presente Modello organizzativo.

Il Responsabile di tali procedure è l'IT Manager, con approvazione e diffusione a carico dell'Amministratore Delegato.

Principi generali e procedure aziendali

Utilizzo della posta elettronica

Le norme di condotta per scambio d'informazioni per via elettronica sono applicabili in particolare a :

- e-mail (posta elettronica) inviata o ricevuta utilizzando computer forniti da ADP Dealer Services Italia s.r.l, oppure nel caso l'utente si presenti, o venga identificato, come un dipendente (i dipendenti vengono denominati associati nelle relative procedure aziendali) di ADP Dealer Services Italia s.r.l;
- accesso ad Internet, mentre si stia utilizzando un computer fornito da ADP Dealer Services Italia s.r.l, oppure nel caso l'utente si presenti, o venga identificato, come un dipendente di ADP Dealer Services Italia s.r.l. Ciò include il collegamento telefonico nei sistemi e nelle reti di ADP Dealer Services Italia s.r.l utilizzando computer di uso privato.

Le norme di condotta di ADP Dealer Services Italia s.r.l impongono che il contenuto della posta elettronica e l'accesso ad Internet si adeguino rigorosamente ai seguenti principi:

- non è permessa posta elettronica o l'accesso a siti internet che contengano materiale pornografico o materiale di natura sessuale esplicita;
- non è permessa posta elettronica o l'accesso a siti internet che violi leggi internazionali, nazionali o locali in materia di pornografia, molestie, diritti civili, diritti d'autore, sicurezza e riservatezza, e/o qualsiasi altra legislazione che si riferisca a mezzi di comunicazione elettronica;
- non è permessa posta elettronica o l'accesso a siti internet, che possa violare le norme di condotta stabilite da ADP Dealer Services Italia s.r.l per quanto riguarda informazioni esclusive o confidenziali;
- non è permesso l'uso della posta elettronica con il data base residente su sistemi diversi dal proprio desktop o laptop;
- qualsiasi incidente collegato alla sicurezza dei dati (per esempio: furto, manomissione di dati, intrusioni e/o tentativi di intrusione) deve essere immediatamente comunicato, non appena scoperto, al Direttore di linea, Direttore HR, e a IIS.
- gli associati devono assicurarsi che non vengano introdotti virus nei sistemi aziendali a seguito di informazioni ricevute via posta elettronica, scaricate da Internet o residenti su supporti removibili (i.e.: dischetti, CD, Memory Key).
- l'uso della posta elettronica a fini personali è accettabile se il livello di utilizzazione è limitato e responsabile.

In aggiunta alle norme di condotta per lo scambio di informazioni per via elettronica, che controllano il contenuto della posta elettronica, vengono raccomandate anche le seguenti linee guida:

- messaggi ricevuti da mittenti sconosciuti devono essere immediatamente cancellati. In particolare non devono essere aperti allegati di alcun genere inseriti in e-mail provenienti da sconosciuti e/o di dubbia origine;
- posta elettronica in arrivo che violi le regole stabilite nelle norme di condotta sullo scambio di informazioni per via elettronica deve essere immediatamente eliminata;
- nel caso si scopra che la posta elettronica in arrivo contenga delle informazioni che violino le norme di condotta, il destinatario deve inviare un messaggio di posta elettronica, richiedendo al mittente di interrompere l'invio di messaggi all'indirizzo del destinatario. Nel caso il destinatario abbia dei problemi oppure riceva qualcosa di offensivo, deve informare immediatamente il Direttore di linea ed il Direttore HR;
- messaggi di posta elettronica in uscita e diretti ad un indirizzo Internet non possono essere considerati sicuri. Il personale deve tenere presente la possibilità che messaggi di posta elettronica contenenti, ad esempio, informazioni confidenziali od esclusive concernenti ADP Dealer Services Italia s.r.l, possano essere intercettati e porre ADP Dealer Services Italia s.r.l in una posizione di svantaggio competitivo. Bisogna valutare sempre se la posta elettronica sia il mezzo adatto a cui affidare il proprio messaggio;
- messaggi di posta elettronica in uscita e diretti ad un indirizzo Internet possono essere persi. Qualsiasi tipo d'informazione che deve arrivare entro un dato limite di tempo, dovrebbe essere inviata via posta elettronica assieme ad un appropriato meccanismo di conferma di ricevuta. Ciò può essere ottenuto mediante l'uso di fax, servizi postali;

- è permessa un'utilizzazione limitata della posta elettronica per uso personale, purché non ci siano interferenze nelle responsabilità professionali dell'individuo, diminuzioni della produttività e tutte le altre linee guida siano rispettate.

Internet è uno strumento importante di ricerca e raccolta d'informazioni. L'accesso ad Internet per scopi personali è ammesso, fermo restando che il livello d'uso deve essere limitato e responsabile.

È bene ricordare che l'accesso remoto è molto costoso e dovrebbe essere limitato a motivi di lavoro. In aggiunta alle norme di condotta sullo scambio d'informazioni per via elettronica (vedi sopra), si raccomanda l'applicazione delle seguenti linee guida:

- è fatto divieto di scaricare qualsiasi programma (software) da Internet, sia esso Freeware, Shareware o Trial senza PREVENTIVA autorizzazione di IIS, da richiedere tramite il modulo di cui all'allegato 3, inviato a mezzo e-mail, allegando tutta la documentazione relativa alle condizioni di licenza, con evidenza della data a cui dette condizioni si riferiscono. In caso di autorizzazione all'uso di software Shareware, l'utilizzatore dovrà rispettare i termini di scadenza e conseguentemente provvedere a regolarizzare la posizione proponendo l'acquisto o cancellando il programma;
- l'accesso a qualsiasi sito internet deve ottemperare alle norme sullo scambio d'informazioni per via elettronica (vedi sopra);
- l'accesso ad internet viene fornito ad ogni dipendente e gestito da apposito software di *web filtering* con gradi di libertà (download tempi di navigazione, etc....) dipendenti dall'attività svolta e dal ruolo ricoperto.
- Durante la navigazione in internet dovrà essere posta la massima attenzione alle precauzioni inerenti i livelli di sicurezza adottati. In particolare, bisognerà:

- avere sempre attivo un firewall software (non necessario per il personale interno se il collegamento avviene tramite LAN);
- avere sempre attivo l'antivirus aggiornato all'ultima versione disponibile;
- in caso di collegamento via WEB alla propria casella personale di posta elettronica non scaricare materiale di dubbia origine o da siti non riconosciuti come attendibili;
- evitare di aprire allegati provenienti da sconosciuto o, comunque, di dubbia origine.

L'accesso limitato ad internet per scopi personali è ammesso, purché non ci siano interferenze nelle responsabilità professionali dell'individuo e siano rispettate tutte le altre linee guida: tale accesso, se necessario, può essere controllato o interdetto da ADP Dealer Services Italia s.r.l.

Ciascun dipendente deve ritenersi responsabile ed assicurarsi che il materiale di ADP Dealer Services Italia s.r.l non venga smarrito o rubato. Sono compresi nei diritti di proprietà di ADP Dealer Services Italia s.r.l, informazioni elettroniche e stampate che siano ottenibili tramite l'uso dei computer.

Tutti i file e i documenti conservati su di un elaboratore (anche portatile) fornito da ADP Dealer Services Italia s.r.l, sono di esclusiva proprietà di ADP Dealer Services Italia s.r.l e dalla medesima controllabili.

Protezione dei dati

Personal computer

Ogni dipendente che utilizzi un personal computer (sia laptop sia altre tipologie), assegnatogli dall'azienda in modo esclusivo, dovrà adottare i seguenti accorgimenti:

- (a) per i soli desktop inserire la password di accensione del BIOS (facoltativo), che evita l'accesso al computer da parte di altre persone, e la password di accesso al Sistema

Operativo Windows (sia utente che Administrator), che evita l'accesso alle informazioni contenute nel sistema;

(b) mantenere segrete le password e non comunicarle, per alcun motivo, ad altre persone.

Comunicare le password esclusivamente, per motivi di sicurezza, a IIS, a mezzo busta chiusa (siglata sui lembi per assicurarne la riservatezza) utilizzando il modulo di cui all'allegato 2;

(c) modificare le password con cadenza periodica (con particolare riferimento alla password utente, il cui rinnovo è richiesto automaticamente dal sistema ogni 45 giorni), e comunque non superiore a 6 mesi (3 mesi per i sistemi che contengono dati "sensibili") secondo le modalità stabilite da IIS, nonché ogniqualvolta siano venute a conoscenza di altre persone (incluso IIS);

(d) utilizzare password composte da almeno 8 caratteri di lettere e numeri, non contenenti alcun riferimento facilmente riconducibile al dipendente;

(e) per i soli laptop è obbligatoria la criptazione del PC utilizzando il software Safeguard.

La password, minimo 8 caratteri alfanumerici, di cui almeno uno maiuscolo o minuscolo, dovrà essere cambiata con la frequenza sopra menzionata. E' a cura di ogni assegnatario conservare copia del kernel generato durante la fase di criptazione su cd non riscrivibile. Il file (xy_z.svf: dove x è l'iniziale del nome, y è il cognome e z è il numero di matricola del laptop) è indispensabile per riattivare il PC in caso di crash e/o malfunzionamenti.

In caso di urgenti necessità operative connesse all'uso del suddetto sistema, ADP Dealer Services Italia s.r.l si riserva la facoltà di accedere al sistema fornito in assegnazione.

In tal caso, qualora il dipendente non fosse rintracciabile per richiedere le credenziali di accesso al sistema, il Direttore di linea provvederà a richiedere a IIS la busta contenente

le menzionate informazioni, dandone contestuale comunicazione, via e-mail, al Responsabile IIS e al dipendente. Quest'ultimo al suo rientro, provvederà a cambiare immediatamente le proprie credenziali di accesso e a fornire nuova busta chiusa contenente le suddette informazioni a IIS.

In aggiunta alle suddette protezioni, l'accesso al Dominio ADP attraverso la rete Internet esterna viene protetto tramite autenticazione a mezzo di una chiave RSA , il cui utilizzo è specificato nell'allegato 8. Il rilascio della chiave RSA è soggetto alla Procedura Assegnazione Beni Aziendali

Server

L'accesso a sistemi server di utilizzo comune (ad esempio: di R&D, F&A, Call Center, etc.) sarà regolato come segue:

- (a) deve essere individuato un responsabile del server ed un suo sostituto, a cura del Direttore di struttura, che provvederà a comunicarlo a IIS. Detti responsabili saranno gli unici ad avere permessi di amministrazione con proprie credenziali utente. L'utente Administrator dev'essere disabilitato. Al fine di garantire il massimo livello di sicurezza il numero di amministratori deve essere ridotto al minimo necessario e concordato con IIS se superiore a due;
- (b) l'accesso al server deve essere protetto da password che ne impedisca l'accesso a persone non autorizzate. Le norme che regolano l'uso e la conservazione delle password sono le medesime di cui al precedente punto (personal computer);
- (c) tutti gli utilizzatori del server avranno inizialmente assegnato un proprio login con relativa password, che sarà loro cura cambiare:
 - immediatamente all'atto dell'assegnazione;
 - successivamente, con periodicità non superiore a sei mesi;

- ogni qualvolta sia venuta a conoscenza di altre persone.

(d) .

Sicurezza Informatica

(a) Ogni stazione di lavoro, sia client che server, deve essere dotata di Antivirus e di apposito programma per il monitoraggio del software e dell'hardware installato al fine di garantire ciascun dipendente e ADP Dealer Services Italia s.r.l nei riguardi del rispetto delle norme sulla tutela della proprietà intellettuale; entrambi i tools dovranno essere configurati ed utilizzati secondo le indicazioni fornite da IIS.

(b) In aggiunta al punto precedente, ogni stazione di lavoro non collegata stabilmente alla rete aziendale di Vigenza deve essere dotata di un personal firewall (fornito di base con il sistema, come ad esempio Windows XP, o con altra soluzione software a parte) configurato secondo le indicazioni fornite da IIS.

(c) Il personale esterno che in visita alla sede centrale di Vigenza avesse necessità di collegarsi alla rete interna, dovrà preventivamente verificare che il proprio PC sia aggiornato con l'ultima versione di antivirus disponibile (fare riferimento alle mail in proposito inviate da IIS). Qualora la versione installata non fosse allineata con l'ultima rilasciata, dovrà preventivamente aggiornarsi utilizzando la connessione telefonica (es. GPRS). Prima di collegarsi alla rete, ogni dipendente dovrà comunque compilare il "Registro Utilizzatori Rete Lan Personale Esterno" (allegato 4) presente nella sala riunione "Padova".

(d) Il personale che abbia necessità di collegare il proprio PC alla rete di un cliente o di un fornitore dovrà verificare preventivamente che il proprio PC sia aggiornato con l'ultima versione di antivirus disponibile, abbia attivato il firewall software e siano messe in atto tutte le precauzioni per evitare intrusioni e/o corruzioni del proprio PC.

(e) E' fatto obbligo a tutti gli associati rispettare le indicazioni e le metodiche sulla sicurezza indicate da IIS, con particolare riferimento agli aggiornamenti relativi all'antivirus. In particolare gli associati collegati alla rete interna di Busa devono essere dotati di Antivirus configurato in modo che il suo aggiornamento avvenga in modalità automatica. Per gli associati non collegati alla rete interna ADP Dealer Services Italia s.r.l, è obbligatorio il costante aggiornamento dell'antivirus secondo le indicazioni fornite da IIS e, comunque, secondo i suggerimenti del fornitore.

Tutti gli associati dovranno effettuare una scansione antivirus del proprio PC almeno una volta al mese, e comunque ogni qualvolta richiesto da IIS o in caso di funzionamenti anomali del sistema.

(f) Periodicamente, ed almeno ogni tre mesi, la rubrica ed i contatti di Outlook devono essere ripuliti da tutti i riferimenti aziendali a personale non più alle dipendenze ADP Dealer Services Italia s.r.l (indirizzi del dominio ADP Dealer Services Italia s.r.l, numero telefono cellulare aziendale etc.).

(g) L'aggiornamento dei Service Pack del Sistema Operativo deve essere effettuato solo previa formale richiesta a IIS o a fronte di sua specifica indicazione.

(h) L'aggiornamento delle patch di Windows (Windows Update) viene effettuata in modo automatico per tutti gli utenti collegati al dominio, ma deve comunque essere controllata, a cura di ogni utilizzatore del sistema almeno una volta al mese.

(i) L'evoluzione delle tecnologie delle comunicazioni mette a disposizione sempre nuovi sistemi e metodologie di connessione, come ad esempio collegamenti a larga banda (i.e. ADSL), apparati wireless (es. Wi-Fi) etc. Questi, se non opportunamente configurati, possono essere fonte di possibili intrusioni, con pesanti conseguenze sulla sicurezza dei dati e delle comunicazioni.

Chiunque utilizzi tali collegamenti e/o apparati con apparecchiature ADP Dealer Services Italia s.r.l deve richiederne preventiva autorizzazione a IIS, che provvederà a fornire tutte le indicazioni e suggerimenti per la loro attivazione in sicurezza.

(j) I palmari utilizzati dagli associati e sincronizzati con altre funzionalità del PC aziendale devono essere protetti da password secondo le indicazioni già fornite al precedente punto 3.1, al fine di evitare indebite intrusioni ai dati in esso contenuti.

(k) La rete aziendale interna dev'essere protetta da possibili intrusioni secondo le indicazioni fornite da IIS in base alle guidelines provenienti dall'HQ ed adeguata secondo le evoluzioni che si rendono necessarie nel tempo.

(l) Qualsiasi attività di variazione alla struttura e/o configurazione della rete interna dev'essere effettuata, e/o autorizzata preventivamente, da IIS.

(m) I collegamenti di Telemaintenance, con qualsiasi interlocutore vengono effettuati, devono essere effettuati senza l'utilizzo di modem ma attraverso gli opportuni canali di collegamento specificati da IIS.

(n) Ogni acquisto di unità centrali deve prendere le dotazioni minime software specificate nei punti precedenti.

(o) Necessità di acquisto di software ed hardware devono essere preventivamente autorizzate da IIS al fine di controllarne l'eventuale disponibilità interna e la rispondenza agli standard definiti.

(p) Il software acquistato deve essere consegnato a IIS che provvederà a registrarne la licenza nel database aziendale, custodirne la relativa documentazione di licenza e a consegnarlo al richiedente; l'acquisto del software è disciplinato dalla Procedura Acquisti.

(q) Una volta installato, il supporto originale deve essere consegnato a IIS, che provvederà a custodirlo in modo appropriato.

(r) E' responsabilità dell'utilizzatore usare il software coerentemente alle indicazioni di licenza indicate dal produttore.

(s) Ogni dipendente che non utilizzi un software fornito in dotazione deve rimuoverlo dalla propria stazione di lavoro e darne immediatamente comunicazione a IIS, che provvederà ad aggiornare il database aziendale e a renderlo disponibile agli altri associati.

(t) Il software licenziato è, di norma, relativo ad una specifica release/versione di prodotto. E' fatto assoluto divieto aggiornare la versione del software senza essere in possesso della relativa licenza di upgrade. Il mancato rispetto della presente norma è equiparabile all'uso di software non licenziato.

(v) Non è consentito all'utilizzatore dei sistemi aziendali ricevuti in assegnazione di modificare le caratteristiche impostate sul PC senza la preventiva autorizzazione di IIS.

(w) E' assolutamente vietato effettuare transazioni bancarie e/o finanziarie (home banking, acquisti on-line e similari) utilizzando l'account aziendale. Eventuali deroghe devono essere autorizzate da HR e IIS.

(x) E' vietata la registrazione a siti i cui contenuti non siano legati all'attività lavorativa utilizzando l'account aziendale, così come l'utilizzo di chat lines, forum non utilizzati a scopo lavorativo bacheche elettroniche etc.

(y) ADP Dealer Services Italia s.r.l fornisce ai propri clienti soluzioni software utilizzando strumenti avanzati di distribuzione del software (distribuzione software su supporti magnetici, via web, ...). Al fine di evitare la distribuzione di software alla clientela contenente virus informatici, dopo la generazione dei supporti / ambiente di

distribuzione dev'esser attentamente verificato, a cura della Delivery, che l'ambiente di rilascio non contenga virus e/o altri componenti che possano alterare, distruggere, modificare i sistemi e/o i dati base dei clienti.

(z) E' fatto assoluto divieto di intercettare file e/o comunicazioni, e, più in generale, usare software e/o hardware in violazione delle norme sulla proprietà intellettuale e sulla privacy.

(aa) L'hardware e il software in dotazione ad ogni dipendente viene inventariato e gestito da IIS. E' fatto assoluto divieto di effettuare trasferimenti di hardware e/o software tra associati, e/o strutture aziendali, senza la preventiva autorizzazione di IIS.

(bb) Con periodicità trimestrale IIS provvederà ad effettuare verifiche campionarie sui sistemi forniti in assegnazione agli associati, al fin di verificarne la coerenza tra quanto utilizzato (software ed hardware) e quanto contenuto nel data base aziendale gestito da IIS.

(cc) Qualsiasi bene aziendale dimesso deve essere consegnato a IIS compilando opportunamente il modulo di "Assegnazione Temporanea Beni Aziendali" con cui è avvenuta la presa in carico. Per i PC e/o Servers dimessi deve essere rimossa ogni password presente ed effettuata una preventiva formattazione a basso livello delle unità di memorizzazione, o un ripristino totale del sistema, per evitare la divulgazione di possibili informazioni riservate. Il sistema deve essere restituito utilizzando l'apposito modulo allegato alle procedure di sicurezza informatica.

Funzione dell'OdV

Tutti i dipendenti ai quali sono assegnati strumenti informatici devono sottoscrivere il documento denominato Procedura di Sicurezza Informatica che si impegnano a rispettare in ogni suo punto.

L'OdV può in ogni momento e senza alcun preavviso procedere alle verifiche su tutta la strumentazione informatica di proprietà di ADP Dealer Services Italia s.r.l in uso al personale e, qualora riscontrasse violazioni al presente Modello ovvero alla Procedura di Sicurezza Informatica, può procedere al ritiro immediato dalla medesima.

Il responsabile della sicurezza informatica deve redigere annualmente una relazione nella quale deve dare opportuna conoscenza all'OdV delle eventuali violazioni rilevate, dei potenziali rischi e delle possibili soluzioni preventive da attuare.

PARTE SPECIALE 4

I reati contro la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/2001)

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la P.A.. Si descrivono brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 agli artt. 24 e 25.

- Malversazione a danno dello Stato o dell'Unione Europea (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 italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

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

Tale ipotesi di reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi,

finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità europea.

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

- 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. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal D.Lgs. 231/2001; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ambito di applicazione del D.Lgs. 231/2001 stesso, nell'ipotesi in cui un dipendente od un agente della società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la società).

- Corruzione per 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 dell'offerente).

L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

- 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.

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

Tale ipotesi di reato si configura nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).

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

L'articolo in esame prevede l'irrogazione di pene in capo a chi da o promette denaro o altre utilità ad un pubblico ufficiale o ad un incaricato di pubblico servizio affinché lo stesso compia un atto d'ufficio o contrario ai doveri d'ufficio.

- Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (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 (oppure ad altro Ente Pubblico o all'Unione Europea).

Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), 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.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

- 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. In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

Aree a rischio

Dall'analisi dei rischi effettuata con la dirigenza ADP Dealer Services Italia s.r.l, è emerso che non sussistono rischi concreti di commissione dei suddetti reati in quanto la società non ha alcun rapporto con pubbliche amministrazioni, enti pubblici e incaricati di pubblico servizio ad eccezione delle visite ispettive da parte degli Enti Pubblici preposti ai controlli di legge (ad es. Agenzia delle Entrate, Asl, *etc.*) in ordine alle quali si riscontra un rischio di grado basso, ma anche perchè esistono una Procedura di Tenuta della Cassa, una Normativa Generale Sistemi di Incentivazione, una Normativa Specifica Piani Incentivi, una Procedura Richieste di Assunzione ed una Procedura Assegnazione Beni Aziendali (già all. sub..) che qui si richiamano come parte integrante del presente Modello Organizzativo, che rendono praticamente impossibile la creazione di fondi “neri” ovvero illeciti favoritismi.

Principi generali, procedure aziendali e soggetti interessati

Non è prevista una procedura aziendale specifica ai contatti con i pubblici funzionari in occasione delle visite ispettive degli enti preposti ai controlli di Legge, tuttavia la reception della Sede di ADP Dealer Services Italia s.r.l. è informata del fatto che le uniche persone titolate a ricevere funzionari pubblici in visita (sia essa ispettiva o per altre ragioni) sono: il legale rappresentante, o, in sua assenza, il Responsabile del Servizio Prevenzione e Protezione, il Direttore Amministrativo e Finanziario e il Direttore HR, i quali dovranno tenere un comportamento corretto e idoneo a favorire gli accertamenti del Pubblico Ufficiale, senza nulla nascondere di quanto a propria conoscenza.

Tutto ciò che riguarda il rapporto con il Pubblico Ufficiale deve essere riportato in un verbale, contenente la copia della documentazione eventualmente rilasciata

dall'Ufficiale, redatto e sottoscritto dalla persona che per conto di ADP Dealer Services Italia s.r.l ha seguito la vicenda.

Nel caso in cui un pubblico ufficiale dovesse per qualsivoglia motivo entrare in rapporto con la società (ispezioni, accertamenti, perquisizioni, sequestri ecc.) di tale visita deve essere data immediata notizia all'OdV, che riceverà altresì copia del verbale sopra menzionato.

PARTE SPECIALE 5

I reati ambientali (D.L.vo 03/04/2006 n. 152 - Art. 192)

Divieto di abbandono

“L'abbandono e il deposito incontrollati di rifiuti sul suolo e nel suolo sono vietati.

È altresì vietata l'immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee.

Fatta salva l'applicazione della sanzioni di cui agli articoli 255 e 256, chiunque viola i divieti di cui ai commi 1 e 2 è tenuto a procedere alla rimozione, all'avvio a recupero o allo smaltimento dei rifiuti ed al ripristino dello stato dei luoghi in solido con il proprietario e con i titolari di diritti reali o personali di godimento sull'area, ai quali tale violazione sia imputabile a titolo di dolo o colpa, in base agli accertamenti effettuati, in contraddittorio con i soggetti interessati, dai soggetti preposti al controllo. Il Sindaco dispone con ordinanza le operazioni a tal fine necessarie ed il termine entro cui provvedere, decorso il quale procede all'esecuzione in danno dei soggetti obbligati ed al recupero delle somme anticipate.

Qualora la responsabilità del fatto illecito sia imputabile ad amministratori o rappresentanti di persona giuridica ai sensi e per gli effetti del comma 3, sono tenuti in solido la persona giuridica ed i soggetti che siano subentrati nei diritti della persona stessa, secondo le previsioni del decreto legislativo 8 giugno 2001, n. 231, in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni.”.

A norma del comma IV del presente articolo la società è chiamata in solido al proprio amministratore o rappresentante che non osservi il divieto previsto.

Il rischio di commissione di reati con riferimento a tale specifica area di rischio viene stimato basso, in quanto non si sono mai verificati inconvenienti né sono mai state contestate infrazioni. Si ritiene opportuno, tuttavia, introdurre una specifica procedura aziendale, volta alla prevenzione di tale tipologia di reati.

La società ADP Dealer Services Italia s.r.l, che provvede allo smaltimento dei propri rifiuti ordinari rispettando la differenziazione indicate dalla normativa comunale applicabile e servendosi degli strumenti forniti dallo stesso ente comunale, si serve di distinte società per lo smaltimento dei rifiuti “speciali”, selezionate a cura dell’IIS Health/Safety manager, nonché Responsabile del Servizio di Prevenzione e Protezione,, Responsabile di tale specifica procedura aziendale, il quale ne verifica previamente l’idoneità e l’iscrizione negli appositi albi, conservando e trasmettendo la relativa documentazione all’OdV.

Il primo tipo di rifiuto “speciale” sono le cartucce per stampanti (toner ed *ink-jet*):

- la società che smaltisce tali rifiuti è la Cooperativa Sociale Il Grillo;
- è chiamata dalla società mediamente ogni mese;
- al ritiro del materiale da smaltire la società rilascia un modulo su carta intestata contenente le seguenti informazioni: la ditta e l'indirizzo del ritiro, il numero dei colli, il peso del materiale, il nome dell'operatore della società che effettua il ritiro e il codice del rifiuto (16.02.16).

Il secondo tipo di rifiuto “speciale” consiste in computer, monitor, stampanti guasti o comunque obsoleti, arredi e materiali vari di volume consistente:

- le società che smaltiscono tali rifiuti sono le ditte Levio Loris e La Rosa;
- sono chiamate dalla società una o due volte l’anno;

- al ritiro del materiale da smaltire rilasciano un modulo sul quale vengono descritti sommariamente i rifiuti ritirati.

La società ADP Dealer Services Italia s.r.l ha individuato il dipendente Gianni Ruffa quale addetto allo smaltimento rifiuti che dovrà:

- contattare i citati fornitori quando lo riterrà necessario secondo il consumo e le esigenze della società;
- assistere alle operazioni di ritiro dei rifiuti;
- controfirmare le ricevute rilasciate dai fornitori attestandone la veridicità;
- redigere apposito verbale con le ricevute e trasmetterlo annualmente al IIS & Health/Safety Manager.

Il IIS & Health/Safety Manager avrà cura di accertare l'attendibilità del verbale confrontandolo con i consumi degli anni precedenti e con gli eventi societari (traslochi, modifiche della struttura, sostituzioni apparecchi *hardware* e *software*) e dovrà sottoscriverlo per accettazione trasmettendone copia all'OdV.