MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

PARTE GENERALE

IP SERVICES S.R.L.

INTEGRATA CON LE LINEE GUIDA ANTITRUST E ANTICORRUZIONE

SOMMARIO

INTRODUZIONE 4
PREMESSA 4
1.1 Il Decreto Legislativo n. 231/2001 e successive modifiche e integrazioni 4
1.2 I reati presupposto 7
1.3 Le sanzioni previste dal D.lgs. 231/2001 16
1.4 Le Linee Guida di Confindustria 18
IL MODELLO 20
2.1 Finalità del Modello 20
2.2 Elementi del Modello 20
2.3 Destinatari del Modello 21
2.4 Approvazione e modifica del Modello 21
2.5 Attuazione del Modello 22
GLI ELEMENTI DEL MODELLO 23
3.1 Protocollo descrittivo del processo di mappatura delle aree a rischio e dei controlli 23
3.2 Il Sistema organizzativo e autorizzativo 24
3.3 Principi di controllo 24
3.4 Il Sistema procedurale 26
3.5 Linee Guida Anticorruzione 26
3.6 Linee Guida Antitrust 28
3.7 Sistema di gestione della privacy 30
3.7.1. Premessa 30
3.7.2. Registro delle attività di trattamento 31
3.7.3 Responsabile della protezione dati 32
3.7.4 Procedura di data breach 34
3.7.5 Titolari, responsabili e persone autorizzate al trattamento sotto l'autorità diretta del titolare o del responsabile 34
3.7.6 Informative e Consensi 36
3.8 Protocollo per l'adozione e l'aggiornamento del Codice Etico 37
3.9 Il Sistema di gestione delle risorse finanziarie 38
3.10 Il Sistema disciplinare 41
3.11 L'Organismo di Vigilanza 44
3.12 Il Sistema di flussi informativi da e verso l'Organismo di Vigilanza 48
3.13 Flusso informativo nei confronti dell'Organismo di Vigilanza 49
3.14 Piano di formazione e comunicazione 51
3.15 Comunicazione del Modello 53
3.16 Prestazione di servizi da o verso altre società 53
3.17 Informativa ai Collaboratori esterni ed ai Partner 54
PRINCIPI, VALORI ETICI E NORME GENERALI DI COMPORTAMENTO 54
4.1 Norme generali di comportamento nei rapporti con la Pubblica Amministrazione 55
4.2 Norme generali di comportamento nei rapporti commerciali 55
4.3 Norme generali di comportamento nella redazione dei bilanci e dei documenti contabili 55
4.4 Conflitti di interesse 55
4.5 Tutela del capitale sociale e dei creditori 55
4.6 Norme generali di comportamento nella gestione dei pagamenti 55
4.7 Norme generali di comportamento per il contrasto al terrorismo 56
4.8 Norme generali di comportamento per la salvaguardia dell'ambiente 56
4.9 Norme generali di comportamento per la tutela della salute e della sicurezza nei luoghi di lavoro 56
4.10 Norme generali di comportamento nell'utilizzo delle tecnologie informatiche 56
4.11 Norme generali di comportamento per il contrasto del riciclaggio 56
4.12 Norme generali di comportamento nei rapporti con l'autorità giudiziaria 56
4.13 Risorse umane 57
4.14 Tutela della concorrenza e dei consumatori 57
4.15 Tutela della privacy e della riservatezza 57

INTRODUZIONE

La società IP Services S.r.l. ha per oggetto le attività di seguito riportate e previste dallo Statuto della Società: il commercio di carburanti, GPL, metano per autotrazione, lubrificanti, elettricità per autotrazione, pneumatici, accessori, ricambi per auto, articoli per automobilisti, autotrenisti, motociclisti e di prodotti alimentari, bevande, articoli da regalo, tabacchi, articoli per fumatori, giornali, riviste, riparazione e lavaggio auto e comunque ogni altro servizio e prodotto commerciabile nell'ambito delle stazioni di servizio in gestione secondo le normative vigenti. La gestione di punti vendita carburanti, stradali ed autostradali, ristoranti, snack bar, officine meccaniche e può compiere ogni operazione dipendente e connessa a tale attività. La società può compiere tutte le operazioni commerciali, industriali, mobiliari, immobiliari, finanziarie, bancarie attive e passive, necessarie od utili, anche indirettamente, per il conseguimento dell'oggetto sociale. La società può, inoltre, assumere interessenze e partecipazioni in altre società o imprese, costituite o costituende, aventi analogo oggetto sociale, connesso od affine al proprio e prestare fideiussioni a garanzia di obbligazioni assunte da terzi.

PREMESSA

1.1 Il Decreto Legislativo n. 231/2001 e successive modifiche e integrazioni

In data 8 giugno 2001, con il Decreto Legislativo n. 231 (di seguito denominato il "Decreto"), entrato in vigore il 4 luglio 2001, il Legislatore ha recepito nel nostro ordinamento quanto stabilito nelle convenzioni internazionali in materia di responsabilità delle persone giuridiche.

Il Decreto, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", ha introdotto un regime di responsabilità amministrativa a carico degli enti, che si aggiunge alla responsabilità penale della persona fisica che ha materialmente commesso il reato.

L'indicazione, nel Decreto, di "responsabilità amministrativa" è formalmente esatta, anche se, sostanzialmente, la natura delle gravi sanzioni previste e la valutazione da parte dello stesso Giudice penale che tratta il processo a carico dell'imputato indicano trattarsi di una forma di responsabilità strettamente legata alla responsabilità penale della persona fisica in ragione dell'appartenenza del fatto reato nella sua dimensione oggettiva all'ente. La responsabilità dell'ente ai sensi del D.L.vo 231/2001 costituisce così un *tertium genus* rispetto a responsabilità penale e responsabilità amministrativa e converge con la responsabilità penale della persona fisica. La responsabilità dell'ente è strettamente collegata alla commissione di un reato, tanto che il fatto di reato di cui risponde la persona fisica è anche fatto dell'ente che risponde del peculiare illecito di cui al D.L.vo 231/2001. Trattandosi di fatto appartenente ad entrambi, persona fisica e persona giuridica, lo schema è quello della responsabilità concorsuale che si articola diversamente in relazione alla diversa natura dei soggetti chiamati a rispondere del medesimo fatto.

La responsabilità dell'Ente sorge soltanto in occasione della realizzazione di determinati tipi di reato da parte di soggetti legati a vario titolo all'ente medesimo e solo nell'ipotesi che la condotta illecita sia stata realizzata nell'"interesse o a vantaggio" di esso: non soltanto, quindi, allorché il comportamento illecito abbia determinato un vantaggio, patrimoniale o meno per l'ente, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il fatto-reato trovi ragione nell'interesse dell'ente.

La Relazione governativa che accompagna il Decreto chiarisce che il richiamo all'interesse dell'ente caratterizza «in senso marcatamente soggettivo la condotta (...) della persona fisica» e si "accontenta" di una verifica *ex ante*. Viceversa, il vantaggio, che può essere tratto dalla società anche quando l'autore del fatto non abbia agito nel suo interesse, richiede sempre una verifica *ex post*.

Gli enti possono essere ritenuti responsabili per alcuni reati commessi o tentati, nel loro interesse o vantaggio da:

a) persona fisica che rivesta funzioni di rappresentanza, amministrazione, direzione, anche di un'unità organizzativa dell'ente dotata di autonomia finanziaria e funzionale;

b) persone che esercitino, anche in via di fatto, la gestione o il controllo dell'ente stesso;

c) soggetti sottoposti alla direzione o vigilanza di chi gestisce o controlla l'ente.

La responsabilità degli enti è indipendente da quella della persona fisica che ha realizzato il fatto nell'interesse o a vantaggio dell'ente stesso. Essa, infatti, sussiste anche quando l'autore del reato non sia stato identificato o non sia imputabile e quando il reato si estingua per una causa diversa dall'amnistia.

Il D.lgs. n. 231/2001 ha diversificato il sistema di responsabilità dell'ente a seconda che il reato sia stato commesso da un soggetto in posizione apicale o da un soggetto sottoposto alla direzione o alla vigilanza di un soggetto in posizione apicale.

È opportuno precisare che l'ente non risponde, per espressa previsione legislativa (art. 5, comma 2, del D.lgs. n. 231/2001), se i soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi.

Nelle ipotesi in cui il reato sia stato commesso da **soggetti in posizione apicale** (sono considerati tali i soggetti specificati nelle lettere a) e b) del presente paragrafo), l'imputabilità all'ente è presunta.

L'art. 6, comma 1, del Decreto prevede che, qualora il reato sia commesso dagli apicali, l'ente non risponde se prova che:

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

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

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

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

Qualora il reato sia stato realizzato da un **soggetto in posizione subordinata** (ovvero da uno dei soggetti descritti nella lettera c) del presente paragrafo), l'onere probatorio è, a differenza di quanto visto nel caso degli apicali, a carico dell'autorità giudiziaria secondo la regola ordinaria che caratterizza il processo penale. L'ente sarà responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza (art. 7, comma 1 d.lgs. 231/2001). In ogni caso, si presume *iuris et de iure* l'osservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi (art. 7, comma 2 d.lgs. 231/2001).

I successivi commi 3 e 4 dell'art. 7 d.lgs. 231/2001 introducono due principi che, sebbene siano collocati nell'ambito della norma sopra rammentata, appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'Ente per entrambe le ipotesi di reato di cui all'art. 5 lettere a) e b). Segnatamente è previsto che:

- il Modello deve prevedere misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione;
- l'efficace attuazione del Modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione; assume rilevanza altresì l'esistenza di un idoneo sistema disciplinare (condizione già prevista dalla lettera *e) sub* art. 6 comma 2).

Sotto un profilo formale, l'adozione e l'efficace attuazione di un Modello non costituisce un obbligo, ma unicamente un onere per gli Enti i quali, invero, potranno anche decidere di non conformarsi al disposto del Decreto senza incorrere per ciò solo in alcuna sanzione.

Tuttavia, l'adozione e l'efficace attuazione di un Modello idoneo è per gli Enti un presupposto irrinunciabile per poter beneficiare dell'esimente prevista dal Legislatore.

È importante, inoltre, considerare che il Modello non è da intendersi quale strumento statico, ma deve essere considerato, di converso, un apparato dinamico che permette all'Ente di eliminare, attraverso

una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali carenze che, al momento della sua creazione, non era possibile individuare.

Ai sensi dell'art. 6, comma secondo del Decreto, il modello organizzativo deve rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi i reati cui si applica la normativa 231;

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

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

d) prevedere obblighi di informazione nei confronti dell'OdV, deputato a vigilare sul funzionamento e l'osservanza del Modello;

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

1.2 I reati presupposto

La responsabilità dell'ente non scaturisce dalla commissione da parte dei soggetti appena individuati di qualsivoglia fattispecie criminosa, ma è circoscritta alle ipotesi di reato previste originariamente dal D.lgs. n. 231/2001 e dalle successive modifiche legislative. Da rilevare, infatti, che il catalogo dei reati c.d. "presupposto" è in continua espansione, come appresso specificato.

Originariamente, il Decreto si riferiva ad una serie di reati commessi nei rapporti con la Pubblica Amministrazione e precisamente:

- indebita percezione di erogazioni pubbliche (art. 316 *ter* c.p.);
- truffa in danno dello Stato o di altro ente pubblico (art. 640, co 2° n. 1, c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640 *ter* c.p.);
- corruzione per un atto d'ufficio (art. 318 c.p., 321 c.p.);
- corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p., 321 c.p.);
- corruzione in atti giudiziari (art. 319 *ter* c.p.);
- corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- concussione (art. 317 c.p.);

malversazione di erogazioni pubbliche (art. 316 *bis* c.p.);

- indebita percezione di contributi, finanziamenti, mutui agevolati o altre erogazioni concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità Europea (art. 316 *ter* c.p.).

Successivamente, l'art. 6 della l. 23.11.2001 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".

L'art. 3 del d.lgs. 11.4.2002 n. 61 ha introdotto, nell'ambito della nuova riforma del diritto societario, il nuovo art. 25 *ter* del Decreto, estendendo il regime di responsabilità degli Enti anche in relazione ai reati societari, così come configurati dallo stesso d.lgs. 11.04.2002 n. 61 (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, aggiotaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza).

Con la l. 14.1.2003 n. 7, è stato esteso il regime di punibilità degli Enti ai reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25 *quater* d.lgs. 231/01).

Con la l. 11.08.2003 n. 228 è stato introdotto l'art. 25 *quinquies* d.lgs. 231/01 con il quale la responsabilità degli Enti viene estesa alla commissione di delitti contro la personalità individuale previsti dalla sezione I del capo XII del libro II del codice penale (riduzione in schiavitù art. 600 c.p.; prostituzione minorile art. 600 *bis* c.p.; pornografia minorile art. 600 *ter* c.p.; detenzione di materiale pornografico art. 600 *quater* c.p.; iniziative turistiche volte allo sfruttamento della prostituzione art. 600 *quinquies* c.p.; tratta e commercio di schiavi art. 601 c.p.; alienazione e acquisto di schiavi art. 602 c.p.).

La l. 18.04.2005 n. 62 (c.d. Legge Comunitaria 2004) e la l. 28.12.2005 n. 262 (c.d. Legge sul Risparmio) hanno esteso il novero dei reati la cui commissione può comportare, ove ne sussistano i presupposti oggettivi e soggettivi, la responsabilità amministrativa degli Enti ai sensi del Decreto.

In particolare, la l. 62/2005 ha introdotto nel corpo del Decreto l'art. 25 *sexies* che prevede la punibilità dell'Ente nel cui interesse o vantaggio siano stati commessi i cosiddetti "*market abuses*" e precisamente i reati di:

- abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 T.U. della Finanza, di cui al d.lgs. 24.2.1998 n. 58);

manipolazione del mercato (art. 185 T.U. della Finanza).

La l. 262/2005 ha, inoltre, previsto all'art. 187 *quinquies* Testo Unico della Finanza una nuova forma di responsabilità dell'Ente conseguente alla commissione nel suo interesse o vantaggio (non di reati ma) degli illeciti amministrativi di:

- abuso di informazioni privilegiate (art. 185 bis T.U. della Finanza);
- manipolazione del mercato (art. 185 ter T.U. della Finanza).

La medesima l. 262/2005, oltre a modificare le norme e le sanzioni (raddoppiando queste ultime) contemplate dall'art. 25 *ter* d.lgs. 231/2001 in materia di reati societari, ha altresì previsto la responsabilità amministrativa degli enti in relazione al reato di omessa comunicazione del conflitto di interessi (art. 2629 *bis* c.c.).

La legge 9.1.2006 n. 7 ha introdotto, nel catalogo dei reati presupposto della responsabilità degli Enti, all'art. 25 *quater*, la nuova fattispecie di pratiche di mutilazione degli organi genitali femminili (art. 583 *bis* c.p.). La norma – evidentemente volta a scoraggiare pratiche di mutilazione poste in essere anche nel nostro Paese per motivi di carattere culturale o religioso – sanziona il fatto di chiunque, in assenza di esigenze terapeutiche, cagiona una mutilazione degli organi sessuali femminili o comunque una lesione degli stessi.

La l. 16.3.2006 n. 146, nel ratificare la Convenzione ed i Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale adottati dall'Assemblea Generale il 15.11.00 ed il 31.5.01 (c.d. Convenzione TOC), ha previsto la responsabilità degli enti per i reati transnazionali di:

- associazione a delinquere (art. 416 c.p.);
- associazione a delinquere di stampo mafioso (art. 416 *bis* c.p.);
- associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 *quater* del T.U. del Presidente della Repubblica del 23.1.1973 n. 43);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 T.U. del Presidente della Repubblica del 9.10.1990 n. 309);
- riciclaggio (art. 648 *bis* c.p.);
- illecito impiego di capitali (art. 648 *ter* c.p.);
- traffico di migranti (art. 12 co 3°, 3 *bis*, 3 *ter*, e 5 del T.U. di cui al d.lgs. 25.7.98 n. 286);
- intralcio alla giustizia, nella forma dell'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'A.G. e del favoreggiamento personale (artt. 377 *bis* e 378 c.p.).

Si definisce reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a 4 anni, qualora in esso sia coinvolto un gruppo criminale organizzato, nonché:

- sia commesso in più d'uno Stato;

sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione e controllo avvenga in un altro Stato;

- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più d'uno Stato;
- ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Il reato transnazionale non costituisce una nuova figura delittuosa introdotta nell'ordinamento italiano, ma rappresenta una qualifica suscettibile di essere applicata a qualsiasi reato già presente nel sistema penale, purché risponda ai requisiti di cui sopra. La stessa Convenzione TOC tuttavia ha imposto agli Stati firmatari di criminalizzare in modo diretto alcuni delitti (quelli specificatamente sopra individuati), più tipicamente transnazionali, al fine di evitare che il solo richiamo alla gravità della pena potesse consentire un'elusione delle pattuizioni convenzionali agli Stati che dovessero punire, nel proprio ordinamento interno, quegli stessi reati con pene inferiori.

La l. 3.8.2007 n. 123 del 2007 ha introdotto l'art. 25 *septies* il quale ha esteso la responsabilità dell'ente ai reati di lesioni colpose gravi e gravissime ed al reato di omicidio colposo commessi in violazione della normativa antinfortunistica. Insieme ai nuovi reati ambientali di natura contravvenzionale (quindi, puniti indifferentemente sia a titolo di dolo che di colpa) contemplati dal nuovo art. 25 *undecies* d.lgs. 231/2001 (inserito dal d.lgs. 121/2011), si tratta degli unici reati commessi a titolo di colpa che possono fondare la responsabilità dell'Ente.

Il d.lgs. 21.11.2007 n. 231 ha introdotto l'art. 25 *octies*, il quale ha esteso la responsabilità dell'Ente ai reati di ricettazione, riciclaggio ed impiego di denaro, beni o altra utilità di provenienza illecita.

Per mezzo della l. 18.03.2008 n. 48 si è poi introdotto l'art. 24 *bis* il quale ha allargato le maglie dei reati presupposto ai delitti informatici e al trattamento illecito di dati. Nello specifico sono stati introdotti i reati di:

- falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491 *bis* c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.);

danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.);

- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 *ter* c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.).

La l. 15.7.2009 n. 94 ha introdotto l'art. 24 *ter* e con esso i delitti di criminalità organizzata:

- associazione per delinquere (art. 416 c.p.);
- associazione per delinquere finalizzata a commettere i delitti di riduzione o mantenimento in schiavitù o in servitù, tratta di persone, acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 d.lgs. 27.7.1998 n. 286 (art. 416, co. 6, c.p.);
- associazione di tipo mafioso (art. 416 *bis* c.p.);
- delitti commessi avvalendosi delle condizioni previste dall'articolo 416 *bis* c.p. per le associazioni di tipo mafioso ovvero al fine di agevolare l'attività di tali associazioni
- scambio elettorale politico-mafioso (art. 416 *ter* c.p.);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, Decreto del Presidente della Repubblica del 9 ottobre 1990, n. 309);
- sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.);
- illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, co. 2, lett. a), n. 5), c.p.p.).

La l. 23.7.2009 n. 99 ha disposto l'introduzione degli artt. 25 *bis.1* e 25 *novies*. Segnatamente, l'art. 25 *novies* ha introdotto i seguenti reati:

- utilizzo dei programmi di *file sharing* per uso personale (art. 171 lett. a *bis* l. 22.4.1941 n. 633);
- reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore e la reputazione (art. 171 co 3 l. 633/941);
- tutela penale del *software* e delle banche dati (art. 171 *bis* l. 633/1941);
- tutela penale delle opere audiovisive o letterarie (art. 171 *ter* l.633/1941);
- responsabilità relative ai supporti (art. 171 *septies* l. 633/1941);
- trasmissioni audiovisive ad accesso condizionato (art. 171 *octies* l. 633/1941).

L'art. 25-*bis*.1 ha introdotto invece i seguenti reati:

- turbata libertà dell'industria o del commercio (art. 513 c.p.);
- illecita concorrenza con minaccia o violenza (art. 513 *bis* c.p.);
- frodi contro le industrie nazionali (art. 514 c.p.);
- frode nell'esercizio del commercio (art. 515 c.p.);
- vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 *ter* c.p.);
- contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 *quater* c.p.).

La l. 3.8.2009 n. 116 ha introdotto l' art. 25 *novies* (poi divenuto art. 25 *decies*, a seguito della modifica apportata dall'art. 2 d.lgs. 7.7.2011 n. 121) che ha esteso la punibilità degli enti anche in caso di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.).

L'art. 2 d.lgs. 7.7.2011 n. 121 ha inserito altresì l'art. 25 *undecies* d.lgs. 231/2001 con il quale sono stati introdotti nella Parte Speciale del Decreto i reati in materia ambientale, e segnatamente:

- il reato previsto dall'art. 727-*bis* c.p., introdotto nel codice dall'art. 1 d.lgs. 121/2011 (uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette);
- il reato previsto dall'art. 733-*bis* c.p., introdotto nel codice dall'art. 1 d.lgs. 121/2011 (distruzione o deterioramento di *habitat* all'interno di un sito protetto);
- i reati previsti dai commi 2 e 3 (rispettivamente, scarico non autorizzato di acque reflue industriali contenenti sostanze pericolose e scarico delle medesime sostanze in violazione delle prescrizioni imposte con l'autorizzazione), 5, periodo primo e secondo (scarico di acque reflue industriali in violazione dei limiti tabellari), 11 (violazione dei divieti di scarico al suolo, nelle acque sotterranee e nel sottosuolo) e 13 (scarico in mare da parte di navi e aeromobili di sostanze di cui è vietato lo sversamento) dell'art. 137 d.lgs. 3.4.2006 n. 152 (T.U. ambientale);
- i reati previsti dai commi 1 lett. *a* e *b* (raccolta, recupero, smaltimento, commercio e intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione), 3, primo e secondo periodo (realizzazione o gestione di una discarica non autorizzata), 4 (inosservanza delle prescrizioni contenute nell'autorizzazione alla gestione di una discarica o alle altre attività concernenti i rifiuti), 5 (miscelazione non consentita di rifiuti) e 6

(deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi) dell'art. 256 d.lgs. 152/2006;

- i reati previsti dai commi 1 e 2 dell'art. 257 d.lgs. 152/2006 (inquinamento del suolo, del sottosuolo, delle acque superficiali e delle acque sotterranee e omissione della relativa comunicazione agli enti competenti);
- i reati previsti dal comma 4, secondo periodo, dell'art. 258 e dai commi 6 e 7 dell'art. 260-*bis* d.lgs. 152/2006 (predisposizione o uso di un falso certificato di analisi dei rifiuti);
- il reato previsto dal comma 1 dell'art. 259 d.lgs. 152/2006 (traffico illecito di rifiuti);
- il reato previsto dall'art. 260 d.lgs. 152/2006 (attività organizzata per il traffico illecito di rifiuti);
- il reato previsto dal comma 5 dell'art. 279 d.lgs. 152/2006 (inquinamento atmosferico);
- i reati previsti dall'art. 1, comma 1 e 2, e dall'art. 2, commi 1 e 2, della l. 7.2.1992 n. 150 (importazione, esportazione, trasporto e uso illecito di specie animali e commercio di piante riprodotte artificialmente);
- il reato previsto dall'art. 6, comma 4, l. 150/1992 (illecita detenzione di esemplari vivi di mammiferi e rettili di specie selvatica o provenienti da riproduzioni in cattività che costituiscano pericolo per la salute o l'incolumità pubblica);
- il reato previsto dall'art. 3-*bis* l. 150/1992 (falsificazione o alterazione di certificazioni e licenze e uso di certificazioni e licenze falsi o alterati per l'importazione di animali);
- il reato previsto dal comma 6 dell'art. 3 l. 28.12.1993 n. 549 (violazione delle disposizioni sull'impiego delle sostanze nocive per lo strato di ozono);
- i reati previsti dagli artt. 8 (inquinamento doloso) e 9 (inquinamento colposo) del d.lgs. 29.12.2007 n. 202 (che dà attuazione alla direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi).

L'art. 2 del d.lgs. 16.07.2012 n. 109 ha introdotto l'art. 25 *duodecies* d.lgs. 231/2001 che prevede tra i reati presupposto l'impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

La legge 6.11.2012 n. 190, ha esteso la responsabilità da reato degli Enti anche ai reati di induzione indebita a dare o promettere utilità e di corruzione tra privati, contemplandoli rispettivamente agli artt. 25, comma 3 e 25 *ter*, comma 1 lettera *s-bis* del decreto.

Il d.lgs. 4.3.2014 n. 39 ha inserito tra i reati presupposto quello di adescamento di minorenni, ora espressamente richiamato dall'art. 25 *quinquies* comma 1 lettera c del Decreto 231.

Con l'art. 3 comma 5 L. 186/2014 è stato modificato l'art. 25 *octies* estendendo la responsabilità degli enti alla nuova fattispecie di autoriciclaggio di cui all'art. 648 *ter*.1 c.p.

L'art. 8 della L. 68/2015 ha modificato l'art. 25 *undecies*, estendendo il catalogo dei reati presupposto della responsabilità amministrativa degli enti con riferimento ai seguenti reati ambientali: inquinamento ambientale (art. 452 *bis* c.p.); disastro ambientale (art. 452 *quater* c.p.); inquinamento ambientale e disastro ambientale colposi (art. 452 *quinquies* c.p.); associazione a delinquere (comune e mafiosa) con l'aggravante ambientale (art. 452 *octies* c.p.); traffico e abbandono di materiale ad alta radioattività (art. 452 *sexies* c.p.).

L'art. 12 della L. 69/2015 ha modificato l'art. 25 *ter*, inasprendo le sanzioni pecuniarie previste per i seguenti reati presupposto della responsabilità amministrativa degli enti: false comunicazioni sociali (art. 2621 e 2621 *bis* c.c.) e false comunicazioni sociali delle società quotate (art. 2622 c.c).

La L. n. 199/2016 ha inserito tra i reati presupposto quello di intermediazione illecita e sfruttamento del lavoro, di cui all'art. 603 *bis* c.p., inserito nell'art. 25 *quinquies*, comma 1, lett. a).

L'art. 6 del d.lgs. n. 38/2017 ha modificato la lettera s-bis) dell'art. 25 ter, inserendo il reato presupposto di istigazione alla corruzione tra privati (art. 2635 *bis* c.c.) ed aumentando la sanzione pecuniaria prevista in relazione al reato di corruzione tra privati (art. 2635 c.c.).

L'art. 30 co. 4 della L. n. 205/2017 introduce sanzioni pecuniarie ed interdittive in relazione alla commissione dei delitti di procurato ingresso illecito e favoreggiamento dell'immigrazione clandestina di cui all'art. 12 del D.lgs. 286/1998.

Da ultimo, l'art. 1 della legge 9 gennaio 2019 n. 3 ha esteso il catalogo dei reati presupposto con riferimento alla fattispecie di cui all'art. 346 bis c.p., traffico di influenze illecite, inserendolo nell'art. 25 del d.lgs. 231/2001.

La L. n. 39/2019 ha introdotto l'art. 25 *quaterdecies* d.lgs. 231/2001 che prevede tra i reati presupposto quelli di frode in competizioni sportive e di esercizio abusivo di gioco o di scommessa (artt. 1 e 4 della l. 401/1989).

La L. 18.11.2019, n. 133 (Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica) ha inserito i reati di cui all'art. 1, comma 11, dello stesso decreto legge nell'art. 24-bis del D.Lgs. 8 giugno 2001, n. 231.

L. 19.12.2019, n. 157 (Conversione in legge, con modificazioni, del decreto-legge 26 ottobre 2019, n. 124, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili) ha modificato l'art. 25-*quinquiesdecies*, introdotto dal D.L. n. 124/2019, introducendo le fattispecie di cui agli artt. 2, 3, 8, 10 e 11 d.lgs. 74/2000.

Il d.lgs. 75/2020 ha disposto la modifica dell'art. 24, comma 1 e l'introduzione del comma 2-bis all'art. 24, nonché la modifica dell'art. 25, comma 1, introducendo le fattispecie di frode nelle pubbliche forniture (art. 356 c.p.), peculato (art. 314 comma 1 e 316 c.p.) e abuso d'ufficio (art. 323 c.p.).

Ha poi disposto la modifica dell'art. 25 *quinquiesdecies*, estendendo la responsabilità amministrativa dell'ente alle fattispecie di cui agli artt. 4 (dichiarazione infedele), 5 (omessa dichiarazione) e 10 quater (indebita compensazione) del d.lgs. 74/2000 se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

Da ultimo, ha introdotto l'art. 25 *sexiesdecies* che estende la responsabilità dell'ente ai reati di cui al D.P.R. 43/1973 (contrabbando).

Il D.Lgs. 8 novembre 2021 n. 184 ha inserito l'art. 25 *octies*1 relativo ai delitti in materia di pagamento con metodi diversi dal contante, introducendo la responsabilità dell'ente in relazione alle fattispecie di cui agli artt. 493 *ter* (Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti) e 493 *quater* (Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti) c.p. e la sanzione pecuniaria sino a 500 quote per il delitto di cui all'articolo 640 *ter*, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale. Ha previsto, altresì, la sanzione pecuniaria a carico dell'ente in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti.

Con il D.Lgs. 8 novembre 2021 n. 195 sono state poi introdotte alcune modifiche alle fattispecie di cui all'art. 25 *octies* D.Lgs. 231/2001.

In particolare, per i reati di ricettazione (art. 648 c.p.), di riciclaggio (art. 648 *bis* c.p.), di impiego di denaro, beni o utilità di provenienza illecita (art. 648 *ter* c.p.) e autoriciclaggio (art. art. 648 *ter* 1 c.p.), è stato ampliato il novero dei reati presupposto alle contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi; per i soli reati di riciclaggio e autoriciclaggio è stata inoltre estesa la loro configurabilità in relazione ai beni provenienti da qualsiasi delitto, anche colposo, come già previsto per le fattispecie di ricettazione e reimpiego.

La legge 9 marzo 2022, n. 22, ha introdotto gli artt. 25 *septiesdecies* – in relazione ai delitti contro il patrimonio culturale di cui agli artt. 518 *bis*, 518 *ter*, 518 *quater*, 518 *octies*, 518 *novies*, 518 *decies*, 518 *undecies*, 518 *duodecies*, 518 *quaterdecies* c.p. – e 25 *octiesdecies* – in relazione alle fattispecie di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici di cui agli artt. 518 *sexies* e 518 *terdecies* c.p.

Per completezza si ricorda che l'art. 23 del Decreto punisce l'inosservanza delle sanzioni interdittive, che si realizza qualora all'Ente sia stata applicata, ai sensi del Decreto medesimo, una sanzione o una misura cautelare interdittiva e, nonostante ciò, lo stesso trasgredisca agli obblighi o ai divieti ad esse inerenti.

L'elenco dettagliato dei reati previsti dal Decreto è allegato al presente Modello (Allegato n. 1).

Tra i reati rientranti nell'ambito di applicazione del d.lgs. n. 231/2001 sono state individuate 13 categorie di reato che appaiono astrattamente suscettibili di essere commessi nell'ambito dell'attività aziendale. Ad esse sono dedicate altrettante sezioni in cui è suddivisa la Parte Speciale del Modello.

Di seguito l'elenco delle categorie di reato astrattamente suscettibili di essere commessi nell'ambito delle attività aziendali:

A) Reati contro la Pubblica Amministrazione;

B) Reati Societari;

C) Reati con finalità di terrorismo, di eversione dell'ordinamento democratico e reati di criminalità organizzata, anche a carattere transnazionale; delitti di contrabbando;

D) Reati contro la personalità individuale;

E) Reati colposi contro l'incolumità individuale commessi con violazione della normativa a tutela della salute e sicurezza dei lavoratori;

F) Reati Informatici;

G) Reati contro l'Industria e il Commercio;

H) Reati in materia di Diritto d'Autore;

I) Reati Ambientali;

J) Reati relativi all'impiego di cittadini di Paesi terzi il cui soggiorno è irregolare;

K) Reati di Ricettazione, Riciclaggio, Impiego di denaro, beni o utilità di provenienza illecita, Autoriciclaggio;

L) Reati Tributari;

M) Delitti in materia di strumenti di pagamento diversi dai contanti.

Occorre, precisare che, a prescindere dall'eventuale Responsabilità Amministrativa dell'ente, chiunque commetta uno dei reati sopra indicati sarà, comunque, perseguibile per la condotta illecita che ha posto in essere.

1.3 Le sanzioni previste dal D.lgs. 231/2001

L'**articolo 9, comma 1, del Decreto** individua le sanzioni che possono essere comminate all'ente per gli illeciti amministrativi dipendenti da reato, ovvero:

1) la sanzione pecuniaria;

2) le sanzioni interdittive;

3) la confisca;

4) la pubblicazione della sentenza.

Da un di vista generale, è opportuno precisare che l'accertamento della responsabilità dell'Ente, nonché la determinazione dell' *an* e del *quantum* della sanzione, sono attribuiti al Giudice penale competente per il procedimento relativo ai reati dai quali dipende la responsabilità amministrativa (art. 36 d.lgs. 231/2001).

L'Ente è ritenuto responsabile dei reati individuati dagli artt. 24 ss. anche se questi siano realizzati nelle forme del tentativo. In tali casi però le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà (art. 26, comma 1 d.lgs. 231/2001).

L'Ente non risponde quando volontariamente impedisca il compimento dell'azione o la realizzazione dell'evento (art. 26, comma 2 d.lgs. 2312001).

Le **"sanzioni pecuniarie"** trovano regolamentazione negli artt. 10, 11 e 12 del Decreto e si applicano in tutti i casi in cui sia riconosciuta la responsabilità dell'Ente. Le sanzioni pecuniarie vengono applicate per quote, in numero non inferiore a 100 e non superiore a 1000, mentre l'importo di ciascuna quota va da un minimo di 258,23 € a un massimo di 1.549,37 €. Il Giudice determina il numero delle quote sulla base degli indici individuati dal primo comma dell'art. 11, mentre l'importo delle quote è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente coinvolto.

Le **"sanzioni interdittive"**, individuate dal comma II dell'art. 9 del Decreto ed irrogabili nelle sole ipotesi tassativamente previste e solo per alcuni reati, sono:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;
- il divieto di pubblicizzare beni o servizi.

Come per le sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinate dal Giudice penale che conosce del processo per i reati commessi dalle persone fisiche, tenendo conto dei fattori meglio specificati dall'art. 14 del Decreto. In ogni caso, le sanzioni interdittive hanno una durata minima di 3 mesi e massima di 2 anni (art. 13, comma 3 d.lgs. 231/2001).

L'art. 1 della legge 9 gennaio 2019 n. 3 ha modificato il comma 2 dell'art. 13, innalzando la durata delle sanzioni interdittive – da 4 a 7 anni se il reato è stato commesso da uno dei soggetti di cui all'art. 5 comma 1 lett. a) e da 2 a 4 anni se il reato è stato commesso da uno dei soggetti di cui all'art. 5 comma 1 lett. b) – in relazione ai delitti di cui all'art. 25 commi 2 e 3 d.lgs. 231/2001, salvo che ricorrano le condizioni di cui al comma 5 bis.

Ai sensi dell'art. 13 del d.lgs. 231/2001, le sanzioni interdittive possono essere applicate all'Ente all'esito del giudizio, accertata la colpevolezza dello stesso, quando ricorre almeno una delle seguenti condizioni:

l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative (art. 13, comma 1 lett. *a*, d.lgs. 231/2001);

- in caso di reiterazione degli illeciti (art. 13, comma 1 lett. *b*, d.lgs. 231/2001).

In virtù dell'art. 45 d.lgs. 231/2001, le sanzioni interdittive possono essere applicate in via cautelare qualora sussistano gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi siano fondati e specifici elementi che fanno ritenere concreto il pericolo di commissione di reati della stessa indole di quello per cui si procede.

La **confisca** del prezzo o del profitto del reato è una sanzione obbligatoria che consegue all'eventuale sentenza di condanna (art. 19 Decreto).

La **pubblicazione della sentenza** è una sanzione eventuale e presuppone l'applicazione di una sanzione interdittiva (art. 18 Decreto).

1.4 Le Linee Guida di Confindustria

Nella costruzione del presente Modello, IP Services S.r.l., oltre all'osservanza delle prescrizioni indicate dal Decreto, ha seguito i principi espressi nelle Linee Guida predisposte da Confindustria (aggiornate a giugno 2021).

Gli aspetti salienti di tali linee (nel seguito denominate "Linee Guida") possono essere così sintetizzati:

a) identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quale area o settore di attività e secondo quali modalità potrebbero verificarsi eventi pregiudizievoli agli obiettivi perseguiti dal D.lgs. n. 231/01;

b) progettazione del sistema di controllo ovvero di protocolli finalizzati a programmare sia la formazione che l'attuazione delle decisioni dell'ente, in relazione ai reati da prevenire.

   Proprio in funzione della realizzazione di tali obiettivi, è stato previsto dalle Linee Guida un sistema di controllo, le cui componenti di maggior rilievo sono:

   i. Codice Etico;

   ii. sistema organizzativo chiaro e formalizzato, con attribuzione di responsabilità, linee di dipendenza gerarchica, descrizione dei compiti e specifica previsione dei principi di controllo adottati;

   iii. procedure manuali e informatiche tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo;

poteri autorizzativi e di firma, con puntuale indicazione dei limiti di approvazione delle spese;

v. sistema di controllo di gestione in grado di segnalare tempestivamente situazioni di particolare criticità;

vi. comunicazione al personale e programma di formazione.

c) individuazione di un Organismo di controllo (l'OdV) della Società con il compito di vigilare sull'efficacia, adeguatezza e applicazione del Modello;

d) l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;

e) disciplina delle modalità di effettuazione delle segnalazioni cd. "whistleblowing";

f) sistema integrato di gestione dei rischi.

2.1 Finalità del Modello

Il presente Modello è finalizzato alla:

a) prevenzione della commissione di uno dei reati di cui al Decreto 231/2001;

b) promozione e valorizzazione in misura ancora maggiore di una cultura etica al proprio interno, in un'ottica di correttezza e trasparenza nella conduzione degli affari;

c) determinazione in tutti coloro che operano in nome e per conto di IP Services S.r.l., della consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;

d) determinazione della consapevolezza che tali forme di comportamento illecito sono fortemente condannate da IP Services S.r.l. in quanto (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono, comunque, contrarie alle disposizioni di legge, ai principi e valori etico-sociali cui IP Services S.r.l. intende attenersi nell'espletamento della propria missione aziendale;

e) introduzione di un meccanismo che consenta di istituire un processo permanente di analisi delle attività aziendali, volto a individuare le aree nel cui ambito possano astrattamente configurarsi i reati indicati dal Decreto;

f) introduzione di principi di controllo a cui il sistema organizzativo debba conformarsi così da poter prevenire, nel concreto, il rischio di commissione dei reati indicati dal Decreto nelle specifiche attività potenzialmente a rischio reato;

g) introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto dei suddetti principi di controllo e, in particolare, delle misure indicate nel presente Modello;

h) istituzione dell'OdV con il compito di vigilare sul corretto funzionamento e l'osservanza del Modello e di curarne il suo aggiornamento;

i) in generale e nell'ottica della integrazione dei sistemi di *compliance*, prevenzione di ogni comportamento o condotta che, pur potendo non determinare la responsabilità amministrativa dell'Ente ai sensi del Decreto, possa integrare un illecito secondo le normative di settore applicabili ad IP Services S.r.l. (quali, ad esempio, illeciti in materia Antitrust o in materia di protezione dei dati personali).

2.2 Elementi del Modello

Il presente Modello si fonda su un insieme integrato di diversi elementi di seguito indicati:

1. Protocollo descrittivo del processo di mappatura delle aree a rischio e dei controlli;
2. Sistema organizzativo e autorizzativo;
3. Principi di controllo relativi alle attività a rischio;
4. Sistema procedurale;
5. Protocollo per l'adozione e l'aggiornamento del Codice Etico;
6. Sistema di gestione delle risorse finanziarie;
7. Sistema disciplinare;
8. Sistema di flussi informativi da e verso l'OdV;
9. Sistema di flussi informativi da e verso il DPO;
10. Linee guida antitrust;
11. Linee guida anticorruzione;
12. Piano di formazione e comunicazione nei confronti del personale di IP Services S.r.l. relativamente alle regole e principi del presente Modello.

Inoltre, il CdA ha affidato il compito di vigilare sul funzionamento e l'osservanza delle regole e dei principi contenuti nel presente Modello e di curarne il suo aggiornamento, ad un organismo dotato di autonomi poteri di iniziativa e di controllo.

2.3 Destinatari del Modello

Le regole contenute nel presente Modello si applicano a tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo in IP Services S.r.l. ai dipendenti, nonché ai consulenti, collaboratori, agenti, procuratori e, in genere, a tutti i terzi che agiscono per conto della Società nell'ambito delle attività considerate "a rischio reato".

I soggetti ai quali il Modello si rivolge sono tenuti, pertanto, a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Società.

2.4 Approvazione e modifica del Modello

L'approvazione del Modello costituisce prerogativa e responsabilità esclusiva del Consiglio di Amministrazione di IP Services S.r.l. (di seguito anche "CdA"). La formulazione di eventuali modifiche e integrazioni del Modello è responsabilità esclusiva del CdA, anche su segnalazione dell'OdV, con riguardo ai seguenti elementi:

- la modifica del documento "Statuto dell'Organismo di Vigilanza" e dei poteri e mezzi dell'OdV;
- l'inserimento/integrazione di principi e valori del Codice Etico;

- modifiche o integrazioni al Sistema disciplinare;
- l'adeguamento e l'aggiornamento del presente Modello.

La responsabilità delle modifiche/integrazioni alla mappatura delle aree a rischio (vedi paragrafo 3.1) e alle procedure organizzative, da considerare parte integrante del Modello, è affidata all'Organo Amministrativo il quale attribuisce all'OdV l'attività di mappatura delle aree a rischio.

Le procedure operative costituiscono elementi di controllo delle attività sensibili, individuate a seguito della mappatura delle aree a rischio. Pertanto, nell'ipotesi di modifica e/o integrazione delle procedure operative, troverà integrale applicazione l'ordinario processo di modifica delle procedure in essere per dare effettiva attuazione a quanto richiesto dal D.lgs. n. 231/2001. Ogni ipotesi o proposta di integrazione e modifica alle procedure del Modello dovrà, pertanto, essere comunicata all'OdV, il quale provvederà anche a darne comunicazione al CdA, nell'ambito del rapporto informativo semestrale.

Relativamente al processo di modifica e aggiornamento della mappatura delle aree a rischio, si rinvia al protocollo descritto nello specifico paragrafo del presente Modello.

Come peraltro chiarito dalle Linee Guida, il CdA, pur con l'istituzione dell'OdV ai sensi del Decreto, mantiene invariate tutte le attribuzioni e le responsabilità previste dal Codice Civile e dallo Statuto della Società, alle quali oggi si aggiungono quelle relative all'adozione e all'efficace attuazione del Modello nonché al funzionamento dell'OdV.

2.5 Attuazione del Modello

L'attuazione del presente Modello è un processo dinamico che ha inizio con l'approvazione del Modello da parte del CdA.

Per la fase di attuazione del Modello, il CdA e l'AD, supportati dall'OdV nei limiti dei propri compiti istituzionali, saranno responsabili, per i rispettivi ambiti di competenza, dell'implementazione dei vari elementi del Modello, ivi comprese le procedure organizzative.

In ogni caso, IP Services S.r.l. intende ribadire che la corretta attuazione e il controllo sul rispetto delle disposizioni aziendali e, quindi, delle regole contenute nel presente Modello, costituiscono un obbligo e un dovere di tutto il personale.

GLI ELEMENTI DEL MODELLO

3.1 Protocollo descrittivo del processo di mappatura delle aree a rischio e dei controlli

L'art. 6, comma 2, lett. a), del Decreto dispone che il Modello deve prevedere un meccanismo volto a "individuare le attività nel cui ambito possono essere commessi reati".

L'individuazione degli ambiti in cui può sussistere il rischio di commissione dei reati implica una valutazione dettagliata di tutti i processi aziendali, volta a verificare l'astratta configurabilità delle fattispecie di reato previste dal Decreto e l'idoneità degli elementi di controllo esistenti a prevenirne la realizzazione. Da questa analisi scaturisce un documento aziendale denominato "mappatura delle aree a rischio e dei controlli" (di seguito denominato "mappatura delle aree a rischio" o "mappatura"), custodito presso la segreteria dell'OdV.

La mappatura delle aree a rischio costituisce il presupposto fondamentale del presente Modello, determinando l'ambito di efficacia e di operatività di tutti i suoi elementi costitutivi.

La predisposizione di tale documento e il suo aggiornamento devono, pertanto, comportare l'implementazione di un vero e proprio processo aziendale che il presente protocollo intende regolamentare.

Di conseguenza, con il presente Modello, IP Services S.r.l. dispone che l'attività di predisposizione e di costante aggiornamento della mappatura delle aree a rischio è responsabilità dell'Amministratore Delegato ed è demandata all'OdV. Quest' ultimo, una volta individuate (con l'eventuale supporto di esperti della materia) le fattispecie di reato astrattamente applicabili alla realtà aziendale, provvede ad effettuare, coadiuvato dal management, un'analisi che assicuri la individuazione delle funzioni aziendali che, in considerazione dei compiti e delle responsabilità attribuite, potrebbero essere coinvolte nelle attività "a rischio reato". Per la descrizione di dettaglio dell'approccio metodologico utilizzato e delle relative risultanze si rimanda **all'Allegato 2 – Mappatura Aree a Rischio**.

Successivamente, i risultati emersi dall'attività di mappatura delle aree a rischio e dei relativi controlli, dovranno essere aggiornati per opera del management aziendale su impulso dell'OdV, anche con l'ausilio di eventuali professionisti esperti nelle tecniche di mappatura, e da questo verificati ogni qual volta incorrano modifiche sostanziali nella struttura organizzativa della Società (per esempio costituzione/modifica di unità organizzative, avvio/modifica di attività di IP Services S.r.l.), oppure qualora intervengano importanti modifiche legislative (per esempio introduzione di nuove fattispecie di reato cui si applica la normativa in esame).

I risultati emersi dall'attività di verifica della mappatura delle aree a rischio e dei relativi controlli, saranno oggetto di specifica comunicazione semestrale da parte dell'OdV al CdA, che provvederà ad assumere le opportune delibere in merito all'aggiornamento del Modello.

3.2 Il Sistema organizzativo e autorizzativo

Il Sistema organizzativo

Come chiarito dalla Linee Guida, il Sistema organizzativo deve essere sufficientemente formalizzato e chiaro, soprattutto per quanto attiene all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e alla descrizione dei compiti, con specifica previsione di principi di controllo, quali per esempio la contrapposizione di funzioni.

Il Sistema autorizzativo

Nel conferimento delle procure la Società prevede che solo i soggetti muniti di formali e specifici poteri possano assumere impegni verso terzi in nome e per conto della Società. Pertanto, le procure permanenti sono conferite unicamente in relazione allo svolgimento di ruoli organizzativi che evidenziano l'effettiva necessità di rappresentanza, tenuto conto delle responsabilità organizzative formalmente attribuite alla struttura di cui il procuratore è parte.

Gli Esponenti aziendali competenti verificano periodicamente il sistema delle procure in vigore, proponendo le necessarie modifiche nel caso in cui le funzioni di gestione e/o la qualifica non corrispondano ai poteri di rappresentanza conferiti.

Nelle Linee Guida viene inoltre chiarito che i poteri autorizzativi e di firma devono essere assegnati in coerenza alle responsabilità organizzative e gestionali definite prevedendo, quando richiesto, una puntuale indicazione delle soglie di approvazione delle spese, specialmente nelle aree considerate "a rischio reato".

Attenendosi ai suggerimenti delle Linee Guida e per quanto di rilevanza ai fini del D.lgs. n. 231/2001, la Società, per il tramite degli Esponenti aziendali competenti, provvede costantemente ad:

- aggiornare l'articolazione dei poteri e il sistema delle procure/deleghe a seguito di modifiche e/o integrazioni delle stesse;
- istituire ed alimentare un flusso informativo formalizzato verso tutti gli Esponenti aziendali, al fine di garantire la tempestiva comunicazione dei poteri e dei relativi cambiamenti;
- effettuare verifiche periodiche sul rispetto dei poteri di firma.

3.3 Principi di controllo

La Società IP Services S.r.l. ha previsto un sistema di controlli incentrato sui principi di seguito rappresentati, così come peraltro previsto nelle Linee Guida di Confindustria.

Si premette, al riguardo, che nell'ambito di ciascuna sezione della parte speciale del modello sopra richiamata, sono state innanzitutto evidenziate le regole generali trasversali a tutti i processi aziendali rilevanti, ossia i principi generali di comportamento cui deve uniformarsi la condotta degli esponenti aziendali nel settore di interesse (ad es., correttezza e trasparenza nella gestione dei rapporti con la Pubblica Amministrazione; gestione degli stessi riservata ai soggetti aziendali autorizzati).

I principi di controllo, che dovranno essere assicurati in tutte le attività "a rischio reato", consistono nel:

- garantire integrità ed etica nello svolgimento dell'attività, tramite la previsione di opportune regole di comportamento volte a disciplinare ogni specifica attività considerata a rischio (per esempio nei rapporti con la P.A.);
- definire formalmente i compiti, le responsabilità di ciascuna funzione aziendale coinvolta nelle attività a rischio;
- attribuire le responsabilità decisionali in modo commisurato al grado di responsabilità e autorità conferito;
- definire, assegnare e comunicare correttamente i poteri autorizzativi e di firma, prevedendo, quando richiesto, una puntuale indicazione delle soglie di approvazione delle spese in modo tale che a nessun soggetto siano attribuiti poteri discrezionali illimitati;
- garantire il principio di separazione dei ruoli nella gestione dei processi, provvedendo ad assegnare a soggetti diversi le fasi cruciali di cui si compone il processo e, in particolare, quella dell'autorizzazione, dell'esecuzione e del controllo;
- regolamentare l'attività a rischio, per esempio tramite apposite procedure, prevedendo gli opportuni punti di controllo (verifiche, riconciliazioni, quadrature, meccanismi informativi, ecc.);
- assicurare la verificabilità, la documentabilità, la coerenza e la congruità di ogni operazione o transazione. A tal fine, deve essere garantita la tracciabilità dell'attività attraverso un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli. È opportuno, dunque, che per ogni operazione si possa facilmente individuare chi abbia autorizzato l'operazione, chi l'abbia materialmente effettuata, chi abbia provveduto alla sua registrazione e chi abbia effettuato un controllo sulla stessa. La tracciabilità delle operazioni è assicurata con un livello maggiore di certezza dall'utilizzo di sistemi informatici in grado di gestire l'operazione consentendo il rispetto dei requisiti sopra descritti;
- assicurare la documentabilità dei controlli effettuati. A tal fine le procedure con cui vengono attuati i controlli devono garantire la possibilità di ripercorrere le attività di controllo effettuate, in modo tale da consentire la valutazione circa la coerenza delle metodologie adottate e la correttezza dei risultati emersi;
- garantire la presenza di appositi meccanismi di *reporting* che consentano la sistematica rendicontazione da parte del personale che svolge l'attività considerata a rischio (report scritti, relazioni, ecc.);
- garantire l'affidabilità del reporting finanziario al vertice aziendale;

prevedere momenti di controllo e monitoraggio sulla correttezza dell'attività svolta dai singoli Esponenti aziendali nell'ambito del processo considerato (rispetto delle regole, corretto utilizzo dei poteri di firma e di spesa, ecc.).

In relazione a ciascuna area a rischio reato o strumentale, sono individuate le modalità con le quali i controlli fondamentali sopra descritti vengono declinati ed attuati in base alle procedure aziendali.

I precetti sopra descritti devono essere rispettati in tutti i processi aziendali e, in particolar modo, nei processi individuati come sensibili.

Sarà responsabilità dell'OdV, per il tramite della funzione di Internal Audit della Capogruppo, verificare che gli Esponenti aziendali competenti provvedano tempestivamente alla verifica e adeguamento dei propri processi ai principi sopra riportati.

L'esito di detto processo di verifica e adeguamento dovrà essere oggetto di specifico *report* periodico da parte delle funzioni aziendali, per quanto di loro competenza, secondo la modalità e la tempistica stabilite dall'OdV stesso.

3.4 Il Sistema procedurale

La Società IP Services S.r.l., in attuazione dei principi sopra descritti, ha implementato il sistema procedurale volto a regolamentare i principali processi aziendali in ottemperanza a quanto richiesto dal D.Lgs. n. 231/2001.

Tale sistema prevede un insieme di procedure aziendali organizzate secondo criteri di codifica descritti e regolamentati dalla procedura di gestione della documentazione, in grado di identificare le procedure adottate allo scopo di prevenire e impedire la commissione dei reati previsti dal Decreto.
Le procedure costituiscono parte integrante del presente Modello.

3.5 Linee Guida Anticorruzione

IP Services S.r.l., in conformità ai principi e valori espressi nel Codice Etico e a quanto previsto dal presente Modello e dalle procedure interne, conduce la propria attività secondo criteri di trasparenza, correttezza e nel rispetto assoluto delle leggi e regolamenti, comunque denominati, finalizzati a prevenire e contrastare la corruzione pubblica e privata.

IP Services S.r.l. richiede, pertanto, a tutti i propri stakeholder di operare in conformità ad ogni normativa applicabile per prevenire e contrastare ogni fenomeno di corruzione.

- Rapporti con la Pubblica Amministrazione – regole di comportamento
  - È vietato a tutti gli esponenti aziendali di corrispondere e offrire, direttamente o indirettamente, denaro o altra utilità di qualsivoglia natura a pubblici ufficiali o incaricati di pubblico servizio al fine d'influenzare o compensare un atto del loro ufficio e/o la omissione o ritardo di un atto del loro ufficio;

- È vietato a tutti gli esponenti aziendali di offrire regali o altre liberalità a funzionari o dipendenti della Pubblica Amministrazione;
- È vietato a tutti gli esponenti aziendali di influenzare, anche per interposta persona, il pubblico ufficiale o l'incaricato di un pubblico servizio nello svolgimento (o per lo svolgimento) di un atto del loro ufficio ovvero per omettere o ritardare un atto del loro ufficio.
- Sono consentiti esclusivamente, nel rispetto delle procedure interne e salvo siano comunque finalizzati ad influenzare l'operato del funzionario pubblico, omaggi o spese di rappresentanza di modico valore e comunque tali da non compromettere l'integrità, l'imparzialità e la reputazione delle parti;
- È fatto obbligo a tutti gli esponenti aziendali di segnalare, anche in forma anonima, ogni possibile violazione della normativa anticorruzione secondo le modalità previste al paragrafo 3.13;
- È fatto obbligo a tutti gli esponenti aziendali di partecipare alla formazione in materia anticorruzione nel rispetto dei programmi e dei contenuti predisposti dalle competenti Funzioni aziendali.

- Rapporti tra privati – regole di comportamento

- È vietato a tutti gli esponenti aziendali sollecitare e/o ricevere denaro o altra utilità di qualsivoglia natura per compiere o per omettere un atto in violazione degli obblighi del loro ufficio/funzione o degli obblighi di fedeltà;
- È vietato a tutti gli esponenti aziendali di praticare favoritismi o porre in essere comportamenti collusivi anche attraverso promesse di vantaggi personali di qualsiasi natura;
- È fatto obbligo a tutti gli esponenti aziendali di segnalare, anche in forma anonima, ogni possibile violazione della normativa anticorruzione secondo le modalità previste al paragrafo 3.13.
- È fatto obbligo a tutti gli esponenti aziendali di partecipare alla formazione in materia anticorruzione nel rispetto dei programmi e dei contenuti predisposti dalle competenti Funzioni aziendali.

IP Services S.r.l. adotterà i provvedimenti disciplinari secondo le previsioni del presente Modello in caso di violazione delle suddette regole di comportamento.

Tutti gli esponenti aziendali devono evitare e comunque segnalare ogni situazione che possa costituire o determinare un conflitto di interesse tra le attività economiche personali e familiari e le mansioni che ricoprono all'interno della Azienda.

Nessun esponente aziendale subirà conseguenze disciplinari (licenziamento, sospensione, demansionamento, trasferimento etc.) o personali per essersi rifiutato di effettuare un pagamento

vietato dalle presenti linee guida, anche se tale rifiuto abbia determinato la perdita di un affare o altra conseguenza pregiudizievole per il business aziendale.

IP Services S.r.l., al fine di prevenire qualsivoglia forma di corruzione, non eroga contributi diretti o indiretti, sotto qualsiasi forma, a partiti, movimenti, comitati, organizzazioni politiche e sindacali, a loro rappresentanti e candidati.

Ogni contributo o iniziativa di beneficienza deve essere preventivamente valutata dalle competenti Funzioni nel rispetto delle procedure interne che disciplinano la gestione dei flussi finanziari e, comunque, secondo criteri di trasparenza e di destinazione delle utilità ad enti affidabili e che operano, a loro volta, secondo criteri di onestà e integrità.

Tutte le attività di sponsorizzazione e pubblicità in genere devono essere effettuate nel rispetto budget approvato e delle procedure interne che disciplinano la gestione dei flussi finanziari.

L'assunzione di personale, di qualsiasi livello, deve avvenire previo espletamento dell'iter di selezione descritto dalle procedure interne. È fatto divieto ad ogni esponente aziendale di proporre alle Funzioni deputate alla selezione ed assunzione del personale figure professionali con le quali siano legati da rapporti di parentela o amicizia.

I contratti con i Partner, Fornitori, Consulenti e Collaboratori esterni devono prevedere l'inserimento e l'accettazione di clausole contrattuali specifiche che li impegnino all'osservanza della normativa anticorruzione e, in generale, di ogni altra normativa al cui rispetto è improntata l'attività di IP Services S.r.l.

3.6 Linee Guida Antitrust

IP Services S.r.l., in conformità ai principi e valori espressi nel Codice Etico e a quanto previsto dal presente Modello e dalle procedure interne, conduce la propria attività nel pieno rispetto delle regole poste a tutela della concorrenza e dei consumatori.

Tutta la popolazione aziendale è tenuta al rispetto delle regole di condotta di seguito indicate, che hanno come obiettivo quello di prevenire la commissione di qualsivoglia illecito antitrust anche attraverso la previsione di idonei canali di comunicazione mediante i quali chiunque venga a conoscenza di violazioni commesse possa darne tempestiva informazione all'Antitrust Compliance Officer della Capogruppo mediante il portale per le segnalazioni *whistleblowing*, utilizzando il link disponibile sul sito www.gruppoapi.com, per la conseguente ed immediata repressione di siffatte condotte secondo quanto previsto dal Modello e dalle procedure interne.

- Riferimenti normativi e condotte vietate

La legge 10 ottobre 1990 n. 287, recante le norme per la tutela della concorrenza e del mercato, vieta alle imprese:

- le intese restrittive della concorrenza, ossia quelle che abbiano per oggetto o per effetto di impedire, restringere o falsare in maniera consistente la concorrenza all'interno del mercato nazionale o in una sua parte rilevante.

Costituiscono intese restrittive della concorrenza gli accordi fra più imprese, in qualsiasi modo conclusi, volti (i) a concertare le condizioni economiche di vendita dei prodotti (ii) a concordare limitazioni nella produzione (iii) a ripartire clienti o territori di vendita (iv) a concordare il rifiuto collettivo di contrattare con un determinato cliente o fornitore (v) a concordare il prezzo massimo o altre condizioni di acquisto nei confronti di un determinato fornitore (vi) a subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari che, per loro natura o secondo gli usi commerciali, non abbiano alcun rapporto con l'oggetto dei contratti stessi. Detti accordi sono da considerarsi nulli ad ogni effetto. Se le intese sono idonee a pregiudicare il commercio tra gli Stati membri, l'Autorità antitrust applicherà la normativa comunitaria (articolo 101 del Trattato sul funzionamento dell'Unione Europea).

- L'abuso di posizione dominante, intendendosi per posizione dominante quella dell'impresa che può comportarsi in modo significativamente indipendente dai concorrenti, dai fornitori e dai consumatori.

La posizione dominante deve essere valutata nel tempo e sulla base della posizione di IP Services S.r.l. nell'ambito del mercato (o mercati) nel quale opera. L'impresa è in posizione dominante, infatti, quando detiene quote elevate in un determinato mercato. La legge non vieta la posizione dominante in quanto tale, ma il suo abuso che si concretizza quando l'impresa sfrutta il proprio potere a danno dei consumatori ovvero impedisce ai concorrenti di operare sul mercato, causando, conseguentemente, un danno ai consumatori. Se l'impresa è in posizione dominante, è fatto quindi divieto (i) di imporre condizioni contrattuali ingiustificatamente onerose (ii) di applicare nei rapporti commerciali con altri contraenti condizioni oggettivamente diverse per prestazioni equivalenti, così da determinare per essi ingiustificati svantaggi nella concorrenza (iii) ostacolare i propri concorrenti (iv) subordinare la vendita di un prodotto all'acquisto di altro non richiesto. Quando l'abuso determina un pregiudizio per il commercio tra più Stati membri dell'UE, l'Autorità applica la normativa comunitaria (articolo 102 del Trattato sul funzionamento dell'Unione Europea).

- Le operazioni di concentrazione, ossia (i) la fusione di due o più imprese prima indipendenti (ii) l'acquisizione del controllo di un'impresa indipendente da parte di una o più imprese (iii) la creazione di imprese comuni.

Non costituiscono invece una concentrazione: le acquisizioni di partecipazioni a fini meramente finanziari; le operazioni infra-gruppo (realizzate fra società controllate, anche se indirettamente, da un unico soggetto); le operazioni i cui partecipanti non svolgono alcuna attività economica. Le operazioni di concentrazione devono essere preventivamente comunicate all'Autorità Garante secondo quanto previsto dalla Legge 287/1990 qualora vengano superate determinate soglie di fatturato. Quando l'Autorità ritiene che una concentrazione comporti la costituzione o il rafforzamento di una posizione

dominante, così da ridurre in modo sostanziale e durevole la concorrenza, ne vieta la realizzazione; l'operazione può anche essere autorizzata subordinatamente al rispetto di talune condizioni, tese a eliminare possibili effetti restrittivi della concorrenza.

Sono altresì vietate le pratiche commerciali scorrette nei confronti dei consumatori, volte a falsarne le scelte economiche, ad esempio, mediante la omissione di informazioni rilevanti, la diffusione di informazioni non veritiere o il ricorso a forme di indebito condizionamento, secondo le previsioni del Codice del Consumo (d.lgs. 206/2005) e di ogni altra normativa nazionale o comunitaria in materia di pubblicità ingannevole e pratiche commerciali scorrette.

- Regole di comportamento

  - È vietato a tutti gli esponenti aziendali di porre in essere qualsiasi condotta che integri o concorra ad integrare gli illeciti descritti al punto che precede;
  - È fatto obbligo a tutti gli esponenti aziendali di segnalare, anche in forma anonima, ogni possibile violazione della normativa Antitrust mediante il portale per le segnalazioni whistleblowing, utilizzando il link disponibile sul sito www.gruppoapi.com; le segnalazioni verranno gestite dall'Antitrust Compliance Officer della Capogruppo in conformità alle procedure interne;
  - È fatto obbligo a tutti gli esponenti aziendali di coinvolgere preventivamente la Funzione Compliance della Capogruppo per la valutazione di conformità normativa di ogni iniziativa di business che possa integrare un'operazione di concentrazione o, in generale, un comportamento potenzialmente rilevante secondo quanto descritto al punto che precede;
  - È fatto obbligo a tutti gli esponenti aziendali di partecipare alla formazione in materia Antitrust nel rispetto dei programmi e dei contenuti predisposti dalle competenti Funzioni aziendali.

IP Services S.r.l. adotterà i provvedimenti disciplinari secondo le previsioni del presente Modello in caso di violazione delle suddette regole di comportamento.

3.7 Sistema di gestione della privacy

3.7.1. Premessa

Il Regolamento del 27 aprile 2016, "General Data Protection Regulation" (di seguito solo "GDPR"), pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, operativo ed applicato, in via diretta, in tutti i Paesi membri dell'Unione Europea dal 25 maggio 2018, persegue il fine di rafforzare la protezione dei dati personali delle persone fisiche, sia all'interno che all'esterno dei confini europei, dunque, si propone di armonizzare le regole privacy di tutti gli Stati membri.

Il GDPR è costituito da tre principi ispiratori, che permeano e sostengono l'intero impianto normativo ed il cui rispetto è protetto da un sistema sanzionatorio, delineato dagli artt. 83 e ss., cui si aggiungono le sanzioni penali previste dalla normativa nazionale, rivista alla luce del D.lgs n.101 del 10 agosto 2018 (pubblicato in G.U. il 4.9.18).

Tali principi essenziali sono quelli di:

- accountability, ossia il principio di responsabilizzazione (art. 32 GDPR).

Si tratta di una innovazione, rispetto all'impostazione precedente, in quanto viene attribuito ai Titolari il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative ed alla luce di alcuni criteri specifici indicati nel Regolamento. Ciò impone un approccio integrato, che interessi tutte le aree aziendali, concreto e risk-based e che dia luogo a comportamenti proattivi.

- privacy by design, che impone l'adozione di misure di protezione fin dalla fase di progettazione del trattamento (art. 25 GDPR).

- privacy by default, che prescrive un utilizzo che si limiti, per impostazione predefinita, ai dati personali necessari (e sufficienti) a rispondere alle finalità specifiche della gestione dei dati e per il periodo strettamente necessario a tali fini (art. 25 GDPR). Tali principi ispiratori si riflettono sui cosiddetti "pilastri" del GDPR, ossia sulle principali novità operative quali:

- l'istituzione del Registro delle attività di trattamento (art. 30);
- la designazione del Responsabile della protezione dei dati (RDP o Data Protection Officer, artt. 37-39);
- il processo di data breach (artt. 33 e 34).

3.7.2. Registro delle attività di trattamento

La Società, in linea con quanto previsto dal Regolamento Europeo 2016/679, ha adottato il registro delle attività di trattamento dei dati personali.

Tale strumento - che costituisce il punto di partenza per la predisposizione dell'intero impianto documentale - è deputato a raccogliere le evidenze, i controlli ed i processi che consentono di soddisfare l'accountability del sistema privacy e dovrà essere messo a disposizione dell'Autorità Garante tutte le volte in cui venga richiesto.

Il Registro dei trattamenti aziendale è compilato in relazione a ciascuna area dalle figure aziendali specificamente individuate dai referenti interni del titolare.

Tale documento è articolato in sezioni e contiene le seguenti informazioni:

- l'area o la struttura aziendale di riferimento;
- le finalità del trattamento;

- la descrizione delle categorie di interessati e delle categorie di dati personali;
- il termine ultimo previsto per la cancellazione delle diverse categorie di dati;
- le operazioni di trattamento (es: raccolta, estrazione, elaborazione, ecc.);
- le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- il tipo di supporto in cui sono contenuti (se informatico, cartaceo o entrambi);
- INPUT (raccolta dati): se presso l'interessato, oppure no;
- la descrizione degli strumenti elettronici usati;
- le banche dati contenenti i dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative;
- il luogo di custodia dei supporti di memorizzazione;
- le strutture che concorrono al trattamento dei dati;
- il nominativo del Privacy contact o coordinator, nonché di eventuali responsabili esterni, amministratori di sistema e contitolari;
- le istruzioni specifiche per le persone autorizzate al trattamento.

3.7.3 Responsabile della protezione dati

Il Consiglio di Amministrazione della Capogruppo Italiana Petroli S.p.A. ha nominato l'avv. Milena Cirigliano, Responsabile della Protezione Dati ai sensi dell'art. 37 Regolamento 2016/679 UE, con i compiti indicati nell'art. 39 del Regolamento e più nel dettaglio:

- informare e fornire consulenza al Titolare del trattamento o al responsabile interno del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione di responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del Regolamento;
- cooperare con l'Autorità di Controllo (Garante Privacy) e fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui

all'art. 36 ed effettuare, se del caso consultazioni relativamente alle leggi in materia di Privacy presenti nell'ordinamento giuridico italiano.

Al Responsabile della Protezione Dati, nello svolgimento delle proprie mansioni, vengono garantite le risorse necessarie in termini di struttura e budget.

Il Responsabile della Protezione dei Dati svolgerà i compiti descritti con riferimento a tutte le Società del Gruppo, avvalendosi a tal fine delle risorse umane ed economiche assegnate.

Nell'ambito di ciascuna Società del Gruppo il referente interno del Titolare sarà tenuto a fornire al RPD informazioni tempestive sulle modalità del trattamento per garantirne l'effettività e la continuità d'azione. All'uopo il RDP del Gruppo sarà raggiungibile da ciascuna Società, Unità periferica o Stabilimento anche per il tramite dell'indirizzo e-mail dedicato – di cui è garantita adeguata pubblicità mediante pubblicazione sull'intranet aziendale e sugli spazi aziendali dedicati alle comunicazioni – nonché mediante la struttura organizzativa dedicata.

Flussi verso il Responsabile della Protezione Dati

Il RDP deve essere coinvolto in tutte le questioni che potrebbero incidere sul corretto trattamento dei dati e, di conseguenza, il Titolare o il Responsabile devono garantire che il RDP:

- partecipi regolarmente alle riunioni tenute dal vertice gerarchico della struttura, ove si prospetti la trattazione di questioni che incidano sul trattamento dati;

- sia presente nel momento in cui vengono prese decisioni che impattano sul trattamento e sulla protezione dei dati (in questo caso al RPD devono essere trasmesse tempestivamente tutte le informazioni necessarie affinché gli sia consentito di fornire una consulenza adeguata);

- sia tempestivamente consultato qualora vi sia un dubbio, si verifichi una violazione dei dati personali o qualsiasi altro incidente che possa incidere sugli stessi (data breaches);

- riceva con cadenza almeno semestrale tutte le informazioni afferenti le modalità del trattamento dei dati da parte dei referenti interni delle Società del Gruppo.

Tutti i pareri e le indicazioni forniti dal RPD devono essere documentati e presi in considerazione. Allo stesso modo, in caso di disaccordo, devono essere documentate le ragioni che hanno portato i vertici dell'organizzazione a non seguire le indicazioni del RPD.

Flussi dal Responsabile della Protezione Dati

Il RPD deve predisporre una informativa periodica per il Consiglio di Amministrazione, contenente:

- la descrizione dei controlli in essere sul trattamento dei dati che hanno impatto sul corretto funzionamento e sull'adeguata osservanza del MOGC adottato dalle singole Società del Gruppo;

- la descrizione della regolarità e della completezza dei flussi informativi relativi alle singole Società del Gruppo;

la indicazione di eventuali modifiche normative in materia di protezione dei dati al fine di agevolare l'aggiornamento del Modello;

- la descrizione generale delle misure di sicurezza tecniche e organizzative implementate, anche in ottica di prevenzione di reati informatici;

- la rendicontazione sull'utilizzo delle risorse assegnate;

- la indicazione di eventuali controversie insorte con privati;

- la informativa circa i controlli espletati in relazione alle violazioni riscontrate;

- la elencazione dei rapporti con l'Autorità Garante in relazione alle richieste preliminari effettuate ai sensi dell'art. 17 del Codice Privacy (rischi specifici rispetto al trattamento dati), ovvero ai sensi della analoga previsione di cui all'art. 36 del GDPR (consultazione preventiva nel caso in cui il RDP abbia indicato al Titolare un rischio specifico rispetto ad un determinato trattamento dei dati); in relazione alle informazioni trasmesse ai sensi dell'art. 157 del Codice Privacy (richiesta di informazioni da parte del Garante); in relazione agli adempimenti ex art. 33 del GDPR (data breaches); in relazione alle autorizzazioni richieste ai sensi degli artt. 46 e 47 del GDPR (trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali).

3.7.4 Procedura di data breach

Per data breach si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

L'eventuale ritardo dovrà essere motivato.

Italiana Petroli S.p.A. ha previsto un'apposita procedura relativa alla gestione dei casi di *data breach* cui tutte le società del gruppo dovranno ispirarsi per l'adempimento degli obblighi normativi.

3.7.5 Titolari, responsabili e persone autorizzate al trattamento sotto l'autorità diretta del titolare o del responsabile

Il regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento.

Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l´autorità diretta del titolare o del responsabile" (art. 4, n. 10, GDPR).

All'interno della propria "struttura" privacy, IP Services S.r.l. individua le seguenti figure:

- il Titolare del trattamento;

- il referente interno del Titolare ai sensi del GDPR;

- gli istruiti al trattamento;

- il responsabile esterno;

- gli amministratori di sistema;

- il titolare autonomo del trattamento;

- il contitolare del trattamento;

- gli autorizzati al trattamento.

Titolare del trattamento

Titolare del trattamento, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è la Società - nella persona del Presidente e Amministratore Delegato - cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che i trattamenti di dati personali effettuati siano conformi al Regolamento.

IP Services S.r.l., titolare del trattamento, con apposita nomina dei referenti ha distribuito le istruzioni sui trattamenti al personale aziendale e assimilato che gestisce dati.

Le istruzioni vengono formalizzate in apposito documento e contengono precise indicazioni in ordine alle modalità del trattamento nel rispetto della finalità di raccolta, in ottemperanza a quanto previsto sul piano normativo e in conformità alla Policy interna sul corretto utilizzo dei sistemi informatici aziendali .

Referente interno del Titolare ai sensi del GDPR

Il titolare ha tra i suoi poteri quello di individuare e nominare i Referenti interni del trattamento.

Ogni referente deve attenersi alle istruzioni impartite dal titolare con l'atto di nomina.

Istruiti al trattamento

Ciascun referente interno individua le persone istruite al trattamento.

All'esito dell'assunzione o del cambiamento di mansioni, il nuovo assunto o il dipendente sottoscrive le istruzioni al trattamento in relazione alle mansioni affidategli.

Amministratori di sistema

Gli amministratori di sistema sono figure professionali dedicate alla gestione ed alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali. Sono, pertanto, professionalità chiamate a svolgere delicate funzioni per la sicurezza delle banche dati e delle reti telematiche.

In conformità al provvedimento del Garante in data 27 novembre 2008 sono stati nominati gli amministratori di sistema e custodi delle credenziali per ogni ambiente operativo (Windows, Linux, Mainframe).

La nomina è avvenuta con atto scritto recante gli obblighi conseguenti, nonché l'indicazione delle verifiche periodiche sull'operato dello stesso che il Titolare si riserva.

Esiste un elenco contenente gli estremi identificativi delle persone fisiche amministratori di sistema e le funzioni ad essi attribuite.

Sono indicati i soggetti terzi cui è affidato il trattamento dei dati in out-sourcing con incarico di Amministratore di sistema, con indicazione della tipologia di dati trattati e del referente interno di IP Services S.r.l.

Responsabile esterno del trattamento

Sono designati responsabili esterni del trattamento di dati personali i soggetti (esterni), cui siano affidate attività che implicano il trattamento, per conto e nell'interesse di IP Services S.r.l., di banche dati di proprietà di IP Services S.r.l. medesima.

I Responsabili esterni del trattamento sono nominati dal titolare con specifica indicazione della tipologia di dati trattati e del referente interno di IP Services S.r.l.

Titolare autonomo del trattamento

I titolari autonomi del trattamento con i quali la società ha rapporti rilasciano autocertificazione ai sensi dell'art. 47 d.p.r. 445 del 2000 in ordine alle corrette modalità di gestione del trattamento.

I medici del lavoro sono titolari autonomi del trattamento dei dati.

Contitolare del trattamento

Quando due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento, entrambi sono contitolari del trattamento.

Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza del regolamento.

3.7.6 Informative e Consensi

L'interessato ha il diritto di conoscere per quali finalità e con quali modalità vengano trattati dal Titolare i dati che lo riguardano.

L´informativa (disciplinata nello specifico dagli artt. 13 e 14 del Regolamento) deve essere fornita all´interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l´interessato).

Se i dati non sono raccolti direttamente presso l´interessato, l´informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della

comunicazione dei dati a terzi o all'interessato e deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare:

- la propria identità, quella di un eventuale suo rappresentante e i propri dati di contatto;
- i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente;
- le finalità del trattamento;
- la base giuridica del trattamento;
- il suo interesse legittimo, se quest'ultimo costituisce la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'intenzione di trasferire i dati personali a un paese terzo o a un'organizzazione internazionale;
- il periodo di conservazione dei dati oppure, i criteri utilizzati per determinare tale periodo;
- i diritti degli interessati.

Le informative per la raccolta del consenso al trattamento dei dati - riguardanti, in via esemplificativa la contrattualistica, la compilazione delle buste paga, i sistemi di sorveglianza aziendale – sono redatte in conformità alle previsioni del GDPR.

È prevista un'apposita procedura relativa alla gestione delle richieste di esercizio dei diritti dell'interessato.

3.8 Protocollo per l'adozione e l'aggiornamento del Codice Etico

In ottemperanza ai criteri di buona *governance*, IP Services S.r.l. ha adottato il Codice Etico **(Allegato n. 3 del presente Modello)** con l'obiettivo di garantire il rispetto di determinati principi, valori e regole di condotta che contribuiscono alla prevenzione dei reati previsti dal d.lgs. n. 231/2001, nonché di descrivere i principi e i valori cui informa il proprio agire, quali legalità, integrità, trasparenza e competenza.

Del Codice Etico è assicurata ampia diffusione, anche mediante pubblicazione sul sito web della Società, tale da assicurarne la conoscenza da parte di tutti i destinatari.

Ogni eventuale modifica del Codice Etico è di competenza del C.d.A.

Il Codice Etico si rivolge sia ai soggetti legati direttamente da un rapporto di lavoro dipendente, dai quali IP Services S.r.l. può esigere il rispetto delle disposizioni etiche, sia agli amministratori, consulenti, collaboratori, agenti, procuratori e terzi, che possono svolgere attività per conto della Società, nonché a tutte le Società del Gruppo.

Il Codice Etico, pertanto, è direttamente applicabile anche a quei soggetti nei cui confronti il rispetto dei principi e valori etici può essere contrattualmente pattuito. L'OdV valuta, con il supporto degli Esponenti aziendali competenti, l'opportunità dell'inserimento di specifiche clausole nei contratti che regolamentano il rapporto con detti soggetti alla luce delle attività aziendali potenzialmente esposte alla commissione dei reati.

L'OdV è deputato al controllo circa il funzionamento e l'osservanza del Codice Etico rispetto alle attività specifiche della Società, provvedendo a comunicare tempestivamente ogni eventuale incoerenza o necessità di aggiornamento al C.d.A.

Eventuali dubbi sull'applicazione dei principi, dei valori e delle regole contenute nel Codice Etico, devono essere tempestivamente discussi con l'OdV; parimenti, chiunque venga a conoscenza di violazioni ai principi e valori del Codice Etico o di altri eventi suscettibili di alterarne la portata e l'efficacia, è tenuto a darne pronta segnalazione all'OdV

Nel caso in cui una delle disposizioni del Codice Etico dovesse entrare in conflitto con disposizioni previste nei regolamenti interni o nelle procedure, prevarrà quanto stabilito dal Codice.

3.9 Il Sistema di gestione delle risorse finanziarie

L'art. 6, comma 2, lett. c) del Decreto dispone che i modelli devono prevedere "modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati". La disposizione trova la sua *ratio* nella constatazione che la maggior parte dei reati di cui al d.lgs. n. 231/2001 possono essere realizzate tramite le risorse finanziarie delle società (per esempio la costituzione di fondi extra-contabili per la realizzazione di atti di corruzione).

Le Linee Guida raccomandano l'adozione di meccanismi di procedimentalizzazione delle decisioni che, rendendo documentate e verificabili le varie fasi del processo decisionale, impediscano la gestione impropria delle risorse finanziarie dell'ente.

Al fine di assicurare la corretta gestione delle risorse finanziarie IP Services S.r.l. ha provveduto a far proprie le procedure organizzative di IP S.p.A. che regolamentano i principali processi amministrativo-contabili, delle quali è peraltro assicurata l'attuazione nelle attività svolte *in service* da IP S.p.A.

Dette procedure costituiscono parte integrante del presente Modello e la violazione fraudolenta delle regole in esse previste costituisce motivo per l'applicazione delle sanzioni previste dal Sistema disciplinare del Modello.

Sulle procedure sopra richiamate dovrà essere esercitato il dovuto controllo da parte di tutti gli Esponenti aziendali coinvolti nei processi di gestione delle risorse finanziarie, in nome del principio di responsabilizzazione degli stessi, e degli organi/funzioni di controllo di IP Services S.r.l., tra cui, l'OdV, il quale dovrà dare contezza nelle comunicazioni periodiche al C.d.A. dei controlli effettuati in merito alla conoscenza e alla corretta applicazione delle suddette procedure.

Ogni modifica alle suddette procedure dovrà essere resa nota all'OdV per gli adempimenti di propria competenza ai fini dell'effettiva attuazione del presente Modello.

Corporate *governance*

La società IP Services S.r.l. adotta un assetto di *governance* di tipo tradizionale, con la presenza di un Consiglio di Amministrazione e un Collegio Sindacale, i cui membri vengono nominati dall'Assemblea dei soci.

Nello specifico, di seguito, si trattano i diversi attori presenti nel sistema organizzativo e di controllo adottato dalla Società, specificandone i ruoli e le interrelazioni anche tramite il rinvio a specifici documenti.

Consiglio di Amministrazione

Il Consiglio di Amministrazione (di seguito anche "C.d.A.") della Società è composto da 4 membri ed è competente nella gestione della Società stessa al fine del perseguimento degli obiettivi strategici e del conseguimento dell'oggetto sociale.

Il Consiglio di Amministrazione di IP Services è investito di tutti i poteri di ordinaria e straordinaria amministrazione, esclusi quelli che la legge o lo Statuto societario riservano espressamente all'Assemblea dei soci.

La rappresentanza della Società di fronte a terzi e in giudizio spetta al Presidente del Consiglio di Amministrazione, o, in caso di assenza o impedimento di quest'ultimo, all'Amministratore Delegato.

Gli aspetti relativi alle modalità di nomina degli amministratori, dei requisiti di onorabilità, professionalità e indipendenza, del funzionamento (convocazioni, deliberazioni, rappresentanza della società), nonché le modalità di remunerazione degli stessi, sono disciplinate all'interno dello Statuto di IP Services S.r.l. e, per ogni aspetto ivi non specificamente disciplinato, dalle norme del codice civile cui si rinvia.

Al C.d.A. spetta la valutazione sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile predisposto dai delegati, con particolare riferimento al sistema di controllo interno e alla gestione dei conflitti di interesse, rispetto alla natura e alle dimensioni della Società. In proposito, tale valutazione, al fine di adottare decisioni pertinenti e consapevoli da parte del C.d.A., deve essere supportata da un'adeguata attività istruttoria. Quest'ultima, in IP Services S.p.A. spetta all'OdV.

Collegio Sindacale

Il Collegio Sindacale (di seguito anche "C.d.S.") di IP Services S.r.l. è composto da un membro.

Ai sensi dell'art. 2403 c.c., il C.d.S "vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento".

Il ruolo del C.d.S., ai sensi di legge, è dunque quello di controllo sull'amministrazione. In particolare, il C.d.S. deve:

- verificare che gli amministratori agiscano in modo informato e che, in particolare, prima di ogni riunione del consiglio, siano fornite a tutti i consiglieri adeguate informazioni sulle materie all'ordine del giorno (cfr. art. 2381, co. 1, c.c.);
- verificare che gli amministratori delegati riferiscano al C.d.A. e allo stesso C.d.S. con la periodicità fissata dallo Statuto, sul generale andamento della gestione e sulle operazioni di maggior rilievo;
- valutare, sulla base delle informazioni ricevute dagli organi delegati, l'adeguatezza dell'assetto organizzativo, amministrativo e contabile della Società;
- accertare che siano rispettate le previsioni di cui all'art. 2391 c.c., nell'ipotesi in cui un amministratore abbia un interesse in una determinata operazione e, in particolare, che il C.d.A. motivi adeguatamente le ragioni per la Società dell'operazione (ipotesi di conflitto d'interessi);
- verificare che i piani strategici, industriali e finanziari siano redatti, quantomeno, in tutte le situazioni in cui appaia opportuno (giudizio di opportunità);
- vigilare sull'esecuzione delle delibere assembleari, quantomeno, in ordine all'assenza di contrasto tra tali delibere e gli atti di gestione;
- vigilare sull'effettivo esame da parte degli amministratori in merito al funzionamento dell'OdV *ex* D.lgs. n. 231/2001;
- vigilare sul corretto funzionamento del sistema amministrativo-contabile, nei termini delle procedure e dei metodi adottati (schemi adottati, deposito e pubblicazione), ovvero della completezza e chiarezza delle informazioni fornite nella nota integrativa e nella relazione sulla gestione, e che i singoli processi del ciclo aziendale siano correttamente riflessi nel sistema amministrativo-contabile stesso. Si tratta, pertanto, di fornire la propria lettura sull'andamento della Società ed esprimere i propri rilievi sul modo in cui il bilancio dia conto di tale andamento. Non spetta, invece, al C.d.S. un controllo di tipo analitico sulla generalità dei dati del bilancio e la loro corretta registrazione, che è invece di competenza della Società di Revisione incaricata da IP Services s.r.l.

In merito alla valutazione dell'assetto organizzativo, è bene precisare che per struttura organizzativa si intende il "complesso delle direttive e delle procedure stabilite per garantire che il potere decisionale sia assegnato ed effettivamente esercitato con un appropriato livello di competenza e responsabilità". I requisiti di adeguatezza cui tale struttura deve uniformarsi, sono di seguito sintetizzati:

- conformità alle dimensioni della Società, alla natura e modalità di perseguimento dell'oggetto sociale;
- organigramma aziendale con chiara identificazione delle linee di responsabilità;
- direzione dell'azienda effettivamente esercitata dagli amministratori;

- documentazione di direttive e procedure aziendali e loro effettiva conoscenza;
- personale con adeguata competenza a svolgere le funzioni assegnate.

Per gli aspetti attinenti la nomina e il funzionamento del Collegio Sindacale e per tutto quanto non specificato in questo paragrafo, si rinvia a quanto definito nel documento "Statuti di IP Services S.r.l." nonché alle norme del codice civile.

Organismo di Vigilanza

La Società, nell'ambito dell'adeguamento del proprio sistema di organizzazione e controllo alle disposizioni del D.lgs. n. 231/2001, ha provveduto all'istituzione di un organo cui è attribuito il compito di vigilare sul funzionamento e l'osservanza del modello, garantendone nel tempo l'adeguatezza e il funzionamento.

L'Organismo di Vigilanza (OdV) è un organo collegiale, composto di 3 membri, le cui caratteristiche compiti e funzionamento sono indicate nello "Statuto dell'Organismo di Vigilanza" **(allegato n. 4 al presente Modello)**, approvato dal C.d.A. e nel documento "Regolamento dell'Organismo di Vigilanza" adottato dall'OdV stesso.

La Funzione di Internal Audit

La funzione di Internal Audit (di seguito denominata "IA") della Capogruppo è la funzione deputata ad assistere IP Services S.r.l. al perseguimento degli obiettivi societari, finalizzando l'attività al monitoraggio e al miglioramento dei processi di controllo e di gestione dei rischi.

I principali obiettivi di tale funzione possono essere così riassunti:

- nel controllo del regolare svolgimento delle attività operative;
- nel controllo dell'andamento dei rischi (stima e valutazione dei principali rischi, loro trattamento e monitoraggio);
- nella valutazione dell'affidabilità complessiva dei controlli interni.

Dati gli obiettivi, le attività dell'IA si esplicano prevalentemente nel monitoraggio sul rispetto delle procedure aziendali (anche tramite periodici test sul funzionamento di tali procedure) e delle procure e deleghe conferite, nonché nella verifica dell'avvenuta rimozione delle anomalie riscontrate in merito all'operatività e nel funzionamento dei controlli ("*follow up*").

Ai fini del coordinamento con gli altri attori del controllo, l'IA espleta compiti di accertamento anche con riguardo a specifiche richieste da parte dell'Organismo di Vigilanza e del Collegio Sindacale e mantiene specifici flussi informativi con gli stessi, in particolare, inviando il Piano annuale di audit e i rapporti di audit a ciascun "preposto" al controllo per quanto di loro attinenza.

La Funzione Internal Audit della Capogruppo svolge, inoltre, il ruolo di segreteria dell'Organismo di Vigilanza.

3.10 Il Sistema disciplinare

Il sistema sanzionatorio del presente Modello è un sistema autonomo di sanzioni finalizzato a rafforzare il rispetto e l'efficace attuazione del Modello in conformità a quanto previsto dall'articolo 6, comma 2, lettera e) del Decreto.

L'applicazione delle misure sanzionatorie stabilite dal Modello non sostituisce eventuali ulteriori sanzioni di diversa natura (penale, amministrativa, civile e tributaria) che possano derivare dal medesimo fatto di reato.

L'applicazione delle sanzioni disciplinari prescinde dalla instaurazione e dall'esito di eventuale procedimento penale avviato nei casi in cui la violazione integri un'ipotesi di reato rilevante ai sensi del Decreto.

Ogni violazione del Modello o delle procedure stabilite in attuazione dello stesso, da chiunque commessa, deve essere immediatamente comunicata, per iscritto, all'Organismo di Vigilanza, ferme restando le procedure e i provvedimenti di competenza del titolare del potere disciplinare.

Il dovere di segnalazione grava su tutti i destinatari del presente Modello.

Ricevuta la segnalazione, l'Organismo di Vigilanza deve immediatamente dare corso ai necessari accertamenti, garantendo la riservatezza del soggetto nei cui confronti procede. Le sanzioni per le violazioni delle disposizioni del presente Modello sono adottate dagli organi o dagli Esponenti aziendali che risultano competenti, in virtù dei poteri e delle attribuzioni loro conferiti dallo Statuto o dai regolamenti interni della Società. Valutata la violazione, l'OdV informa immediatamente il titolare del potere disciplinare, che darà corso al procedimento disciplinare di sua competenza al fine delle contestazioni e dell'eventuale applicazione delle sanzioni.

A titolo esemplificativo, costituiscono infrazioni disciplinari i seguenti comportamenti:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, dei principi e delle procedure previste dal presente Modello o stabilite per la sua attuazione;
- la redazione, eventualmente in concorso con altri, di documentazione non veritiera;
- l'agevolazione, mediante condotta omissiva, della redazione da parte di altri, di documentazione non veritiera;
- la sottrazione, la distruzione o l'alterazione della documentazione inerente la procedura per sottrarsi al sistema dei controlli previsto dal Modello;
- l'ostacolo alla attività di vigilanza dell'OdV;
- l'impedimento all'accesso alle informazioni e alla documentazione richiesta dai soggetti preposti ai controlli delle procedure e delle decisioni;
- l'attuazione di condotte ritorsive, discriminatorie e punitive nei confronti del personale autore di segnalazioni di violazioni del sistema dei controlli previsto dal Modello e/o di illeciti;
- l'abuso del potere/dovere di segnalazione, tramite indicazioni false o infondate sulla commissione di illeciti e/o violazioni del Modello di Organizzazione, Gestione e Controllo;

la realizzazione di qualsiasi altra condotta idonea a eludere il sistema di controllo previsto dal Modello;

- la realizzazione di qualsiasi condotta in contrasto con i principi e valori sanciti dal Codice Etico.

Sanzioni e misure disciplinari

Le sanzioni applicabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e la Società, nonché proporzionate alla gravità della violazione valutata alla luce del grado di imprudenza, negligenza, imperizia ovvero intenzionalità della condotta; altresì, alla luce della eventuale reiterazione di comportamenti illeciti, del ruolo e della responsabilità dell'autore, delle mansioni e del grado di autonomia del lavoratore e di ogni altra particolare circostanza del fatto.

Il Modello costituisce un complesso di norme alle quali il personale dipendente deve uniformarsi anche ai sensi di quanto previsto dai rispettivi CCNL in materia di norme comportamentali e di sanzioni disciplinari. Pertanto, la violazione delle previsioni del Modello e delle sue procedure di attuazione, comporta l'applicazione del procedimento disciplinare e delle relative sanzioni, ai sensi di legge e dei citati CCNL. Nei confronti dei lavoratori dipendenti con qualifica di operaio, impiegato e quadro, il sistema disciplinare è applicato in conformità all'art. 7 della legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori) e ai vigenti CCNL applicabili. Qualora il fatto costituisca violazione anche di doveri discendenti dalla legge o dal rapporto di lavoro, tali da non consentire la prosecuzione del rapporto di lavoro neppure in via provvisoria, potrà essere deciso il licenziamento senza preavviso, a norma dell'art. 2119 c.c., fermo il rispetto del procedimento disciplinare.

Le altre sanzioni comminabili ai lavoratori dipendenti sono:

- il rimprovero verbale;
- l'ammonizione scritta;
- multa in conformità alle previsioni del CCNL;
- sospensione dal lavoro e dalla retribuzione in conformità alle previsioni del CCNL;
- licenziamento con preavviso.

In ogni caso verranno applicate tutte le disposizioni e le garanzie previste dal CCNL in materia di procedimento disciplinare.

Il rispetto delle disposizioni del Modello vale nell'ambito dei contratti di lavoro di qualsiasi tipologia e natura, inclusi quelli con i Dirigenti, a progetto, part-time, nonché nei contratti di collaborazione rientranti nella c.d. parasubordinazione. Se la violazione riguarda i Dirigenti, il sistema disciplinare è applicato in conformità alla legge e al CCNL applicabile. Con la contestazione, può essere disposta la revoca di eventuali procure affidate al soggetto interessato.

IP Services S.r.l.– Libro dei Verbali del Consiglio di Amministrazione
Cod. Fisc.: 01180380212

Se la violazione riguarda un Amministratore della Società, l'Organismo di Vigilanza deve darne immediata comunicazione al Consiglio di Amministrazione e al Collegio Sindacale mediante relazione scritta.

Nei confronti degli Amministratori che abbiano commesso una violazione del Modello o delle procedure stabilite in attuazione del medesimo, il Consiglio di Amministrazione può applicare ogni idoneo provvedimento consentito dalla legge, fra cui le seguenti sanzioni, determinate a seconda della gravità del fatto e della colpa, nonché delle conseguenze che sono derivate alla Società:

a) richiamo formale scritto;

b) sanzione pecuniaria pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile;

c) revoca, totale o parziale, delle eventuali procure.

Qualora la violazione dell'amministratore sia tale da ledere la fiducia della Società nei suoi confronti, il Consiglio di Amministrazione convoca l'Assemblea, proponendo la revoca dalla carica.

In caso di violazione da parte di un componente del Collegio Sindacale, l'Organismo di Vigilanza deve darne immediata comunicazione al Consiglio di Amministrazione mediante relazione scritta. Il Consiglio di Amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, propone all'Assemblea l'adozione dei provvedimenti di competenza e provvede agli ulteriori incombenti previsti dalla legge.

In caso di violazione del Modello da parte di uno dei componenti dell'OdV, gli altri membri ovvero i sindaci o gli amministratori ne informano immediatamente il Consiglio di Amministrazione e il Collegio Sindacale, i quali assumono i conseguenti provvedimenti, fra cui la revoca dell'incarico, previa valutazione delle argomentazioni difensive e/o giustificazioni addotte.

Per i soggetti esterni o le controparti contrattuali destinatarie del Modello, secondo quanto previsto dai paragrafi 3.16 e 3.17, l'Organismo di Vigilanza, sentiti gli Esponenti aziendali competenti, stabilisce per ciascuna tipologia di rapporto le misure sanzionatorie applicabili nei casi di violazione delle previsioni del Modello o delle procedure stabilite per la sua attuazione, nonché individua le modalità di applicazione delle stesse. Qualora si verifichino fatti che possono integrare violazione del Modello da parte di questi soggetti, l'Organismo di Vigilanza informa mediante relazione scritta il Consiglio di Amministrazione, il quale, sentiti gli Esponenti aziendali competenti, valuterà le modalità per procedere all'accertamento della violazione.

3.11 L'Organismo di Vigilanza

Il D.lgs. n. 231/2001, all'art. 6, comma 1, lett. b) prevede, tra i presupposti indispensabili per l'esonero dalla responsabilità conseguente alla commissione dei reati, l'istituzione di un organismo interno all'Ente - nel prosieguo denominato "OdV" - dotato di autonomi poteri di iniziativa e controllo, con il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento.

Ai sensi dell'art. 6 comma 2 *bis*, i modelli devono prevedere:

1) adeguati canali informativi che consentano ai soggetti in posizione apicale e ai loro subordinati di presentare segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del decreto, fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente. Tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

2) un canale alternativo di segnalazione, per garantire con modalità informatiche, la riservatezza dell'identità del segnalante;

3) il divieto di atti di ritorsione o discriminatori nei confronti del segnalante per motivi collegati alla segnalazione;

4) adeguate sanzioni nei confronti di chi violi le suddette misure di tutela del segnalante;

5) adeguate sanzioni nei confronti di chi abusi del diritto di segnalazione fornendo indicazioni infondate.

Requisiti dell'Organismo di Vigilanza

L'OdV deve soddisfare i seguenti requisiti:

- autonomia e indipendenza: come anche precisato dalle Linee Guida, la posizione dell'OdV nell'Ente "deve garantire l'autonomia dell'iniziativa di controllo da ogni forma di interferenza e/o condizionamento da parte di qualunque componente dell'Ente" (ivi compreso l'organo dirigente). L'OdV, pertanto, deve essere inserito in una posizione la più elevata possibile con la previsione di un riporto informativo al massimo Vertice operativo aziendale. Inoltre, al fine di garantirne la necessaria autonomia di iniziativa e indipendenza, "è indispensabile che all'OdV non siano attribuiti compiti operativi che, rendendolo partecipe di decisioni e attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello". Si precisa che per "compiti operativi" ai fini del presente Modello e dell'attività di IP Services S.r.l., si intendono le attività che possano ripercuotersi su aspetti strategici o finanziari della Società.
- Professionalità: tale requisito si riferisce alle competenze tecniche specialistiche di cui deve essere dotato l'OdV per poter svolgere l'attività che la norma gli attribuisce. In particolare, i componenti dell'OdV devono avere conoscenze specifiche in relazione a qualsiasi tecnica utile per compiere l'attività ispettiva, di consulenza, di analisi del sistema di controllo e di tipo giuridico (in particolare nel settore penalistico e societario), come chiaramente specificato nelle Linee Guida. È infatti essenziale la conoscenza delle tecniche di analisi e valutazione dei rischi, del *flow charting* di procedure e processi, delle metodologie per l'individuazione di frodi, del campionamento statistico e della struttura e delle modalità realizzative dei reati.
- Continuità di azione: tale requisito deve connotare l'attività dell'OdV per garantire l'efficace attuazione del Modello organizzativo.

Pertanto, quale organo preposto a vigilare sul funzionamento e l'osservanza del Modello e a curarne il continuo aggiornamento, nonché quale organo dotato di specifici poteri di iniziativa e di controllo, l'OdV deve:

- essere indipendente e in posizione di terzietà rispetto a coloro sui quali dovrà effettuare la vigilanza;
- essere dotato di autonomi poteri di iniziativa e di controllo;
- essere dotato di autonomia finanziaria;
- essere privo di compiti operativi;
- assicurare continuità d'azione;
- avere i requisiti di professionalità sopra descritti;
- poter usufruire di un canale diretto di comunicazione con il Vertice aziendale.

Individuazione dell'Organismo di Vigilanza

In attuazione di quanto previsto dal Decreto e dalle Linee Guida e nel rispetto dei requisiti di autonomia, indipendenza, professionalità e continuità d'azione appena illustrati, l'OdV di IP Services S.r.l. è stato individuato in un organo plurisoggettivo. L'OdV di IP Services S.r.l. si compone di 3 membri.

Lo "Statuto dell'OdV" **(allegato n. 4 al presente Modello)**, cui si rinvia per quanto appresso non specificamente riportato, disciplina le modalità e i requisiti per la nomina dei suoi componenti, le cause di incompatibilità, le cause di revoca/cessazione dal mandato, compiti e poteri di ciascun membro e dell'Organo nella sua collegialità. Disciplina, altresì, le caratteristiche e il funzionamento dello stesso.

I componenti dell'Organismo di Vigilanza, a garanzia della loro posizione di terzietà ed autonomia, non devono:

1. intrattenere, direttamente o indirettamente, al di fuori del rapporto di lavoro subordinato, relazioni economiche con la Società, con le sue Controllate, con gli Amministratori esecutivi, con l'azionista o il gruppo di azionisti che controllano la Società, di rilevanza tale da condizionarne l'autonomia di giudizio, valutata anche in relazione alla condizione patrimoniale soggettiva della persona fisica in questione;

2. essere titolari, direttamente o indirettamente, di partecipazioni azionarie di entità tale da permettere di esercitare il controllo o un'influenza notevole sulla Società;

3. essere stretti familiari di Amministratori esecutivi della Società o di soggetti che si trovino nelle situazioni indicate nei punti precedenti.

All'atto dell'accettazione dell'incarico, il componente dell'Organismo di Vigilanza rilascia una dichiarazione nella quale attesta l'assenza dei menzionati motivi di incompatibilità.

Inoltre i componenti dell'Organismo di Vigilanza per poter essere scelti e mantenere la carica non devono essere stati condannati, anche con sentenza non ancora divenuta irrevocabile, per avere commesso uno dei reati di cui al D.lgs. 231/2001 ovvero ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o dagli uffici direttivi delle persone giuridiche.

Qualora un soggetto esterno venga nominato componente dell'Organismo di Vigilanza, invia al Consiglio di Amministrazione, all'atto dell'accettazione dell'incarico, una dichiarazione:

1. che attesti l'assenza, in capo a sé, di ragioni ostative ovvero d'inopportunità (conflitti di interesse, rapporti di parentela con Amministratori esecutivi, precedenti penali rilevanti o procedimenti in corso, ecc.) all'assunzione dell'incarico;

2. nella quale dichiari di essere stato adeguatamente informato sulle regole comportamentali ed etiche che la Società ha adottato, ivi comprese quelle contenute nel presente Modello e che egli farà proprie nello svolgimento dell'incarico.

I componenti dell'Organismo di Vigilanza durano in carica il periodo stabilito in sede di nomina e possono essere rieletti, previa verifica esplicita del permanere dei requisiti di eleggibilità più sopra descritti. I componenti dell'Organismo di Vigilanza possono essere revocati soltanto dal Consiglio di Amministrazione, previa informativa al Collegio Sindacale, in caso di:

1. sopravvenienza di una delle cause di incompatibilità di cui sopra;

2. inadempienza reiterata ai compiti previsti dal Modello;

3. inattività ingiustificata che abbia comportato l'applicazione di sanzioni interdittive per la Società.

I componenti dell'Organismo di Vigilanza possono rassegnare in qualunque momento le proprie dimissioni e cessano dall'incarico nel momento in cui tali dimissioni vengano accettate dal Consiglio di Amministrazione, ovvero venga nominato altro componente in sostituzione. In ogni caso dopo un mese dalle dimissioni cessano dalla carica.

La Segreteria dell'Organismo di Vigilanza

L'attività di segreteria dell'OdV è assegnata alla Funzione Internal Audit della Capogruppo IP S.p.A., la quale provvederà ad ogni adempimento necessario al fine di poter dare concreta attuazione a quanto previsto dal presente Modello in capo a tale organismo.

L'OdV e l'interazione con le altre funzioni aziendali.

L'OdV, nello svolgimento dei compiti affidatigli e per le proprie finalità istituzionali, potrà avvalersi inoltre della collaborazione:

1. della funzione di Internal Audit della Capogruppo, per la verifica dei processi gestionali e dell'applicazione delle procedure organizzative emanate in attuazione del presente Modello,

nonché per le attività di identificazione, valutazione e controllo dei rischi di commissione di reati previsti dal D.lgs. n. 231/2001;

2. di altre unità organizzative della Società ovvero della capogruppo IP S.p.A., quali, a mero titolo esemplificativo la Direzione Amministrazione e Finanza (in ordine, per esempio, al controllo dei flussi finanziari);
3. del Dirigente di IP S.p.A. preposto alla redazione dei documenti contabili societari per quanto di competenza;
4. di opportuni supporti esterni, secondo le valutazioni del caso.

Nelle riunioni periodiche, l'OdV invita il DPO al fine di condividere le tematiche di *compliance* integrata nell'ottica di un sistema integrato di gestione dei rischi.

È previsto, inoltre, per il corretto e completo espletamento delle attività di vigilanza, un coordinamento sistematico dell'OdV con le risorse della Società e con le Direzioni aziendali di IP S.p.A. in relazione alle attività svolte in *service*.

3.12 Il Sistema di flussi informativi da e verso l'Organismo di Vigilanza

L'OdV riferisce in merito all'attuazione del Modello e alle eventuali criticità ad esso connesse al Presidente e Amministratore Delegato, al Consiglio di Amministrazione e al Collegio Sindacale.

L'OdV si riunisce con cadenza almeno trimestrale e relaziona:

- su base continuativa con il Presidente e Amministratore Delegato.
- su base periodica nei confronti del Consiglio di Amministrazione e del Collegio Sindacale.

Relativamente a quest'ultima forma di reporting, l'OdV predispone i seguenti rapporti scritti:

1) con cadenza semestrale, relazione di sintesi dell'operato dell'OdV (attività complessivamente svolte, attività non effettuate per giustificate ragioni di tempo e risorse, suggerimenti di interventi correttivi/migliorativi del Modello ritenuti necessari o opportuni e loro stato di realizzazione).
2) con cadenza annuale, i risultati ottenuti dall'attività di verifica svolta e il piano di verifiche previste per il successivo periodo di riferimento.

Gli incontri con gli organi societari cui l'OdV riferisce devono essere verbalizzati e copia dei verbali è custodita dall'OdV stesso nell'apposito archivio secondo le modalità e i tempi da questo stabiliti.

L'OdV potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione e potrà a sua volta presentare richiesta in tal senso, al fine di riferire in merito al funzionamento del Modello e a situazioni specifiche, direttamente e indirettamente inerenti l'applicazione del Modello e/o l'attuazione del Decreto.

Qualora il Dirigente di IP S.p.A. preposto alla redazione dei documenti contabili societari, nell'ambito delle sue competenze, venga a conoscenza di comportamenti, da parte del personale della Società, che

integrino violazioni del Modello e dei suoi elementi, è tenuto a darne tempestiva comunicazione all'OdV.

In ogni caso l'OdV e il Dirigente di IP S.p.A. preposto alla redazione dei documenti contabili societari si riuniscono con cadenza almeno semestrale per la trattazione degli argomenti di cui sopra; della riunione è redatto verbale.

L'OdV deve, inoltre, coordinarsi con le strutture tecniche competenti di IP Services S.r.l. e IP S.p.A., in relazione alle attività svolte in *service*, per i diversi profili specifici.

3.13 Flusso informativo nei confronti dell'Organismo di Vigilanza

L'art. 6, comma 2, lett. d) del D.lgs. n. 231/01 impone la previsione nel Modello di obblighi informativi nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello stesso.

L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto.

Le informazioni fornite all'OdV mirano a migliorare le sue attività di pianificazione dei controlli e comportano un'attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati.

In particolare, oltre alle informazioni specificatamente richieste nelle procedure aziendali, devono essere tempestivamente trasmessi all'OdV, in via esclusiva e riservata, da parte di tutte le funzioni aziendali le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività di indagine per i reati di cui al Decreto, avviate anche nei confronti di ignoti;
- ogni violazione del Modello e dei suoi elementi costitutivi e ogni altro aspetto potenzialmente rilevante ai fini dell'applicazione del Decreto;
- eventi e atti che possano ledere la garanzia di tutela dell'integrità dei lavoratori e ogni altro aspetto in tema di misure antinfortunistiche e di salute e igiene sul lavoro potenzialmente rilevante ai fini dell'applicazione dell'art. 25 *septies* del D.lgs. n. 231/2001;
- rapporti predisposti dagli Esponenti aziendali e dagli organi di controllo nell'ambito delle attività di controllo svolte, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del sistema disciplinare, evidenzianti i procedimenti disciplinari svolti e le eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti nei confronti dei dipendenti), ovvero i provvedimenti motivati di archiviazione dei procedimenti disciplinari;
- ogni eventuale modifica e/o integrazione al sistema di deleghe e procure;
- esistenza di attività aziendali risultate e/o percepite come prive in tutto o in parte di apposita e/o adeguata regolamentazione (assenza totale o parziale di specifica regolamentazione,

inadeguatezza dei principi e valori del Codice Etico e/o delle procedure operative rispetto alle finalità cui sono preordinati, sotto il profilo della chiarezza e comprensibilità, aggiornamento e corretta comunicazione, etc.);

- ogni eventuale emanazione, modifica e/o integrazione effettuata o ritenuta necessaria alle procedure operative concernenti il Modello e il Codice Etico.

Oltre al delineato sistema informativo, che assume valore tassativo, chiunque venga in possesso di notizie relative alla commissione di reati o a comportamenti ritenuti non in linea con quanto previsto dal presente Modello è tenuto comunque a darne immediata notizia all'OdV.

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 di IP Services S.r.l. o delle persone coinvolte, nonché la reputazione del/dei segnalato/i.

Le segnalazioni possono essere effettuate in modalità informatica tramite email, all'indirizzo odvipservices@pec.gruppoapi.com, o mediante il portale per le segnalazioni whistleblowing, utilizzando il link disponibile sul sito internet www.gruppoapi.com. In alternativa possono essere trasmesse al canale tradizionale di posta ordinaria all'indirizzo Segreteria dell'OdV di IP Services S.r.l., c/o Italiana Petroli S.p.A., via Salaria 1322, 00138 Roma (RM).

Le segnalazioni di violazioni non possono in nessun caso comportare ritorsioni a carico dei soggetti segnalanti, né discriminazioni di alcun genere per motivi da collegarsi alla segnalazione.

Si provvederà all'applicazione di congrue sanzioni a carico di coloro i quali, all'interno dell'azienda si rendessero responsabili di comportamenti ritorsivi, discriminatori e/o vessatori a carico degli autori di segnalazioni di illeciti.

È vietato a tutti i dipendenti segnalare violazioni e/o illeciti falsi, infondati abusando del diritto di segnalazione ad essi garantito.

Si provvederà all'applicazione di congrue sanzioni a carico di coloro i quali, all'interno dell'azienda, abusando del potere/dovere di segnalazione, forniscano indicazioni false o infondate sulla commissione di illeciti e/o violazioni del Modello di Organizzazione, Gestione e Controllo.

Distintamente dagli obblighi di comunicazione "tempestiva" sopra tassativamente indicati, con il presente Modello si introduce anche un obbligo di comunicazione semestrale all'OdV che grava in capo a tutte le risorse aziendali specificatamente individuate dall'OdV stesso, ma formalmente designate dal Presidente e Amministratore Delegato con idonea comunicazione organizzativa a firma di quest'ultimo.

In particolare, i soggetti destinatari della suddetta comunicazione saranno tenuti a compilare, con cadenza semestrale, uno specifico report informativo inviatogli dall'OdV e da restituire allo stesso nei tempi da questi stabiliti, contenente:

riferimenti alla risorsa aziendale;

- le aree/attività/processi risultanti dalla mappatura come a rischio in cui la risorsa interviene;
- la richiesta di specifiche informazioni in merito alla permanenza o meno dei requisiti di rischio di dette aree;
- la richiesta di informazioni in merito ad eventuali ulteriori attività a rischio non considerate;
- la richiesta di indicare lo stato di attuazione dei controlli posti a presidio di dette aree a rischio;
- la possibilità di segnalare eventuali suggerimenti di miglioramento circa gli elementi del Modello.

Detto report dovrà contenere una specifica attestazione in merito alla veridicità dei dati e delle informazioni in esso contenute.

Ogni informazione, segnalazione e/o report sono conservati dalla segreteria dell'OdV in un apposito archivio per un periodo di 10 anni. L'accesso all'archivio è consentito esclusivamente ai membri dell'OdV.

3.14 Piano di formazione e comunicazione

La formazione interna costituisce uno strumento imprescindibile per un'efficace implementazione del Modello e per una diffusione capillare dei principi di comportamento e di controllo adottati da IP Services S.r.l. al fine della prevenzione dei reati di cui al D.lgs. n. 231/2001.

A tal fine, la Direzione/Funzione responsabile della gestione delle Risorse Umane di IP S.p.A., in condivisione con l'OdV, promuove la realizzazione di un piano di formazione specifico dei soggetti destinatari del presente Modello, in merito ai contenuti di tale documento e del Decreto.

I requisiti che detto programma di formazione deve rispettare sono i seguenti:

- essere adeguato alla posizione ricoperta dai soggetti all'interno dell'organizzazione (neo-assunto, impiegato, quadro, dirigente, ecc.);
- i contenuti devono differenziarsi in funzione dell'attività svolta dal soggetto all'interno dell'azienda (attività a rischio, attività di controllo, attività non a rischio, ecc.);
- la periodicità dell'attività di formazione deve essere funzione del grado di cambiamento cui è soggetto l'ambiente esterno in cui si colloca l'agire aziendale, nonché della capacità di apprendimento del personale e del grado di *committment* del management a conferire autorevolezza all'attività formativa svolta;
- il relatore deve essere persona competente e autorevole al fine di assicurare la qualità dei contenuti trattati, nonché di rendere esplicita l'importanza che la formazione in oggetto riveste per IP Services S.r.l. e per le strategie che essa intende perseguire;

la partecipazione al programma di formazione deve essere obbligatoria e devono essere definiti appositi meccanismi di controllo per verificare la presenza dei soggetti e il grado di apprendimento di ogni singolo partecipante.

La formazione può essere classificata in generale o specifica. In particolare, la formazione generale deve interessare tutti i livelli dell'organizzazione, al fine di consentire a ogni individuo di:

- conoscere i precetti stabiliti dal D.lgs. n. 231/2001 e di essere consapevole che IP Services S.r.l. intende farli propri e renderli parte integrante della cultura aziendale;
- conoscere gli obiettivi che la Società si prefigge di raggiungere tramite l'implementazione del Modello e le modalità con le quali le mansioni di ciascuno possono contribuire al raggiungimento degli stessi;
- avere cognizione del proprio ruolo e delle proprie responsabilità all'interno del sistema di controllo interno presente in IP Services S.r.l.
- conoscere quali sono i comportamenti attesi o accettabili e quelli non accettabili da IP Services S.r.l;
- conoscere i canali di reporting adeguati al tipo di informazione che si vuole comunicare e al soggetto cui si vuole far arrivare la comunicazione stessa, e, in particolare, sapere a chi segnalare e con quali modalità la presenza di anomalie nello svolgimento delle attività aziendali;
- essere consapevole dei provvedimenti disciplinari applicabili nel caso di violazioni delle regole del presente Modello;
- conoscere i poteri e i compiti dell'OdV e, in conseguenza, gli obblighi informativi nei confronti di tale organismo;

La formazione specifica, invece, interessa tutti quei soggetti che per via della loro attività necessitano di specifiche competenze al fine di gestire le peculiarità dell'attività stessa, come il personale che opera nell'ambito di attività segnalate come potenzialmente "a rischio reato". Questi dovranno essere destinatari di una formazione sia generale che specifica. In particolare, la formazione specifica dovrà consentire al soggetto di:

- avere consapevolezza dei potenziali rischi associabili alla propria attività, nonché degli specifici meccanismi di controllo da attivare al fine di monitorare l'attività stessa;
- conoscere le tecniche di valutazione dei rischi inerenti l'attività da esso svolta nonché le esatte modalità di svolgimento della stessa e/o le procedure che la regolamentano, al fine di acquisire la capacità di individuare eventuali anomalie e segnalarle nei modi e nei tempi utili per l'implementazione di possibili azioni correttive.

Anche i soggetti preposti al controllo interno, cui spetta il monitoraggio delle attività risultate potenzialmente a rischio, saranno destinatari di una formazione specifica al fine di renderli consapevoli delle loro responsabilità e del loro ruolo all'interno del sistema del controllo interno, nonché delle sanzioni cui vanno incontro nel caso disattendano tali responsabilità e tale ruolo.

In caso di modifiche e/o aggiornamenti rilevanti del Modello saranno organizzati dei moduli di approfondimento mirati alla conoscenza delle variazioni intervenute.

Saranno, in ultimo, organizzati specifici moduli per i neoassunti destinati ad operare nelle aree a rischio.

3.15 Comunicazione del Modello

In linea con quanto disposto dal Decreto e dalle Linee Guida, IP Services S.r.l. darà piena pubblicità al presente Modello, al fine di assicurare che il personale sia a conoscenza di tutti i suoi elementi.

La comunicazione dovrà essere capillare, efficace, chiara e dettagliata, con aggiornamenti periodici connessi ai mutamenti del Modello.

Per essere efficace, la comunicazione deve:

- essere sufficientemente dettagliata in rapporto al livello gerarchico di destinazione;
- utilizzare i canali di comunicazione più appropriati e facilmente accessibili ai destinatari della comunicazione al fine di fornire le informazioni in tempi utili, permettendo al personale destinatario di usufruire della comunicazione stessa in modo efficace ed efficiente;
- essere di qualità in termini di contenuti (tale da rendere fruibili tutte le informazioni necessarie), di tempestività, di aggiornamento (deve contenere l'informazione più recente) e di accessibilità.

Pertanto, il piano effettivo di comunicazione relativo alle componenti essenziali del presente Modello dovrà essere sviluppato, in coerenza ai principi sopra definiti, tramite i mezzi di comunicazione aziendali ritenuti più idonei, quali per esempio l'invio di e-mail o la pubblicazione sulla rete aziendale.

3.16 Prestazione di servizi da o verso altre società

IP Services S.r.l. ha attribuito in outsourcing ad IP S.p.A. lo svolgimento di diversi processi che interessano le attività sensibili mappate nel Modello. Ciò sulla base di un contratto di servizi scritto.

Si prevede:

- l'obbligo da parte di IP S.p.A. di attestare la veridicità e completezza della documentazione prodotta o delle informazioni comunicate a IP Services S.r.l. nello svolgimento dei servizi richiesti;

- la determinazione del corrispettivo basata su criteri obiettivi;

- l'obbligo di IP S.p.A. di rispettare, nello svolgimento del servizio richiesto, il Codice etico di Gruppo e le procedure aziendali;

IP Services S.r.l. ha attribuito in outsourcing a società esterne al Gruppo i seguenti processi che interessano le attività sensibili mappate nel Modello:

- vigilanza dei Punti Vendita, recupero, trasporto, contazione e deposito valori;

fattura metrica degli erogatori.

Ciò sulla base di contratti scritti contenenti previsioni analoghe a quelle sopra evidenziate.

Qualora IP Services S.r.l. presti in favore di società appartenenti al Gruppo dei servizi, ciascuna prestazione deve essere disciplinata da un contratto scritto.

Il contratto di servizi deve prevedere le seguenti clausole:

- l'obbligo da parte di IP Services S.r.l. di attestare la veridicità e la completezza della documentazione prodotta o delle informazioni comunicate alla società beneficiaria del servizio ai fini dello svolgimento dei servizi richiesti;

- l'obbligo da parte di IP Services S.r.l. di rispettare nello svolgimento del servizio prestato il Codice Etico e quanto previsto dal presente Modello e dalle procedure stabilite per la sua attuazione. Qualora i servizi erogati rientrino nell'ambito di attività sensibili non contemplate dal presente Modello, la Società si impegna a dotarsi di regole e procedure adeguate e idonee a prevenire la commissione dei reati previsti dal Decreto.

3.17 Informativa ai Collaboratori esterni ed ai Partner

IP Services S.r.l. promuove la conoscenza e l'osservanza dei principi e delle regole di condotta previsti dal Codice Etico e dal presente Modello anche tra i consulenti, i partner, i collaboratori a vario titolo, i clienti e i fornitori. Per tali soggetti saranno, pertanto, predisposti meccanismi per l'inserimento e l'accettazione di clausole contrattuali specifiche che, sentito l'OdV, verranno inserite negli schemi contrattuali di riferimento.

PRINCIPI, VALORI ETICI E NORME GENERALI DI COMPORTAMENTO

Fatto salvo quanto previsto dal Codice Etico (all. 3 al presente Modello) che esprime i principi e i valori che connotano la cultura d'impresa di tutte le Società del Gruppo, IP Services S.r.l. intende ribadire la sussistenza dell'obbligo per tutti i Dipendenti di osservare scrupolosamente le regole di comportamento sotto enucleate. Dette regole hanno una funzione immediatamente precettiva e, per quanto ivi non espressamente normato, integrativa delle procedure interne richiamate nelle Parti Speciali del Modello.

IP Services S.r.l. non giustifica alcun comportamento che, seppure compiuto nel suo interesse e/o a suo vantaggio, contrasti con i principi e valori etici del Codice, con le regole di seguito esposte, con le procedure che disciplinano tutte le attività aziendali e, in generale, con le previsioni del Modello. In ogni caso la violazione di dette regole determinerà la applicazione delle sanzioni disciplinari in conformità al CCNL e al presente Modello.

IP Services S.r.l., nei rapporti con i terzi, darà corso alla immediata risoluzione del contratto qualora gli stessi pongano in essere, nel corso, in ragione o in conseguenza del rapporto, comportamenti

contrari alle regole, ai principi e ai valori cui si ispira nell'agire aziendale anche quando il partner o collaboratore ritenga di agire nell'interesse o a vantaggio di IP Services S.r.l.

4.1 Norme generali di comportamento nei rapporti con la Pubblica Amministrazione

IP Services S.r.l. esige che i propri dipendenti tengano comportamenti corretti nei rapporti con la Pubblica Amministrazione. È quindi fatto divieto di praticare qualsivoglia forma di corruzione, favoritismi, comportamenti collusivi, sollecitazioni dirette e/o indirette anche attraverso promesse di vantaggi personali, nei confronti di qualunque soggetto appartenente alla Pubblica Amministrazione.

È fatto divieto di fornire alla Pubblica Amministrazione informazioni e/o documenti falsi o attestanti cose non vere, ovvero omettere informazioni rilevanti.

4.2 Norme generali di comportamento nei rapporti commerciali

Nei rapporti commerciali con privati e Partner in genere, è vietato fornire informazioni e/o documenti non rispondenti al vero o che omettano notizie rilevanti secondo la natura dell'affare.

4.3 Norme generali di comportamento nella redazione dei bilanci e dei documenti contabili

È fatto obbligo di redigere e tenere le scritture contabili in conformità alle previsioni normative. I bilanci devono contenere informazioni veritiere ed è fatto obbligo di rispettare i principi contabili nell'inserimento delle cd. valutazioni. I rapporti con le Autorità Pubbliche di vigilanza, il Collegio Sindacale, i Soci o la Società di Revisione devono essere improntati a criteri di trasparenza, collaborazione e verità.

4.4 Conflitti di interesse

È fatto obbligo a tutti gli esponenti aziendali di rendere noto qualsiasi conflitto di interesse che sia sorto o possa sorgere in relazione ad uno o più affari. Le comunicazioni dovranno essere precise e dovranno specificare la natura, i termini e l'origine del vantaggio o potenziale vantaggio. In attesa delle valutazioni e decisioni societarie sul punto, gli interessati, siano essi Amministratori o Dipendenti, dovranno astenersi dal compiere qualsiasi operazione.

4.5 Tutela del capitale sociale e dei creditori

È vietato a tutti gli esponenti aziendali di compiere atti simulati o fraudolenti al fine di influenzare la maggioranza dei soci falsando il libero formarsi della volontà dell'assemblea in sede deliberante.

È vietato porre in essere condotte finalizzate alla realizzazione di operazioni illecite sulle azioni o quote sociali anche delle altre Società del gruppo.

È fatto divieto agli Amministratori di effettuare operazioni societarie o sul capitale al fine di cagionare danni ai creditori.

4.6 Norme generali di comportamento nella gestione dei pagamenti

È fatto obbligo di rispettare la normativa vigente e le procedure interne in materia di pagamenti, utilizzo e circolazione di monete, carte di pubblico credito e valori di bollo. È fatto obbligo di garantire la tracciabilità di tutti i pagamenti.

I rapporti e le transazioni infragruppo devono essere adeguatamente regolamentati in forma scritta e i flussi di denaro da o verso altre Società del Gruppo devono essere tracciati e trovare giustificazione nel contratto.

4.7 Norme generali di comportamento per il contrasto al terrorismo

È vietata qualsiasi condotta idonea ad integrare atti di terrorismo o di eversione dell'ordinamento ovvero di finanziamento, diretto o indiretto, di associazioni aventi finalità di terrorismo o di eversione dell'ordine democratico.

4.8 Norme generali di comportamento per la salvaguardia dell'ambiente

È fatto obbligo di rispettare le previsioni normative in materia di tutela dell'ambiente e di operare al fine di evitare o comunque ridurre l'impatto dell'attività aziendale sull'ambiente.

4.9 Norme generali di comportamento per la tutela della salute e della sicurezza nei luoghi di lavoro

È fatto obbligo di rispettare le norme di legge e tutte le procedure interne finalizzate a garantire la salute e la sicurezza nei luoghi di lavoro nel rispetto dei ruoli, della mansioni e delle responsabilità a ciascuno assegnate nell'ambito delle misure organizzative adottate da IP Services S.r.l. per una efficace tutela dei lavoratori dai rischi che possano insorgere nello svolgimento delle loro attività.

4.10 Norme generali di comportamento nell'utilizzo delle tecnologie informatiche

È fatto obbligo di utilizzare le tecnologie informatiche e i dispositivi informatici forniti alla popolazione aziendale nel rispetto delle procedure che ne regolamentano gli usi e, comunque, esclusivamente per finalità lecite connesse allo svolgimento della attività lavorativa.

4.11 Norme generali di comportamento per il contrasto del riciclaggio

È fatto obbligo di rispettare la normativa e le procedure interne finalizzate alla prevenzione del riciclaggio. Sono vietate le condotte che direttamente o indirettamente possano integrare forme di collaborazione con associazioni criminose in genere e di stampo mafioso. È inoltre vietata ogni operazione che possa concretizzarsi in un utilizzo di denaro, beni o utilità di provenienza illecita nonché qualunque attività e/o forma di riciclaggio.

4.12 Norme generali di comportamento nei rapporti con l'autorità giudiziaria

È vietato qualunque comportamento che possa rivelarsi di intralcio alla giustizia. I rapporti con l'Autorità Giudiziaria devono essere improntati a criteri di collaborazione, verità e trasparenza.

4.13 Risorse umane

È vietata ogni forma di discriminazione nei confronti dei Dipendenti per ragioni politiche, sindacali, religiose, razziali, di lingua, di nazionalità, di sesso e di condizioni di salute. È fatto obbligo di rispettare la normativa giuslavoristica e le procedure interne nella gestione delle Risorse Umane, anche nei rapporti con fornitori, appaltatori o partner.

4.14 Tutela della concorrenza e dei consumatori

È fatto obbligo di gestire gli affari e le operazioni societarie nel rispetto della normativa e delle procedure interne a tutela della libertà di concorrenza, del consumatore e del diritto d'autore.

4.15 Tutela della privacy e della riservatezza

È fatto obbligo di rispettare la normativa e le procedure interne a tutela del diritto alla privacy e alla riservatezza. Le informazioni e i dati anche di carattere non personale devono essere trattati dalle persone a ciò autorizzate nel rispetto della suddetta normativa.

ALLEGATI

1) Elenco Reati;
2) Mappatura delle aree a rischio;
3) Codice Etico;
4) Statuto dell'Organismo di Vigilanza.