

Web Consult S.r.l.

Modello di Organizzazione Gestione e Controllo ai sensi del decreto legislativo 8 giugno 2001, N. 231

Approvato dal Consiglio di Amministrazione di
Web Consult S.r.l. nella seduta
del 29/03/2016
Da luglio 2023 è intervenuta la variazione della
denominazione sociale da Web Consult S.r.l. a
Tecnologica S.r.l.

Modello in fase di revisione e aggiornamento

INDICE

Parte Generale

1. IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMATIVA RILEVANTE	8
1.1. Il regime di responsabilità amministrativa previsto a carico delle persone Giuridiche	8
1.2. Sanzioni	12
1.3. Azioni esimenti dalla responsabilità amministrativa	13
2. LINEE GUIDA DI CONFINDUSTRIA	14
3. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE E GESTIONE DA PARTE DI WEB CONSULT S.r.l.	15
3.1. Motivazioni di Web Consult S.r.l. nell'adozione del modello di organizzazione e gestione	15
3.2. Finalità del Modello	16
3.3. Struttura del Documento	17
3.4 Modifiche ed integrazioni del Modello	18
4. ORGANISMO DI VIGILANZA	18
4.1. Identificazione dell'Organismo di Vigilanza	18
4.2. Funzioni e poteri dell'Organismo di Vigilanza	19
4.3. Reporting dell'Organismo di Vigilanza nei confronti degli organi societari	20
4.4. Flussi informativi nei confronti dell'Organismo di vigilanza	20
4.4.1. Segnalazioni da parte di esponenti aziendali o da parte di terzi	20
4.4.2. Obblighi di informativa relativi ad atti ufficiali	21
4.4.3. Sistema delle deleghe	21
5. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE	21
5.1. Introduzione	22
5.2. Diffusione e informazione	22
5.3. Clausole contrattuali	23
5.4. Adozione del Codice Etico e sua diffusione	23
6. SISTEMA DISCIPLINARE E MISURE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO	24
6.1. Principi generali	24
6.2. Sanzioni per i lavoratori dipendenti	24

6.2.1. Quadri, Impiegati, Operai	24
6.2.2. Dirigenti	26
6.3. Misure nei confronti degli amministratori	26
6.4. Misure nei confronti di collaboratori esterni	26
7. CONFERMA APPLICAZIONE E ADEGUATEZZA DEL MODELLO	26

Parte speciale "A"

Reati in danno della Pubblica Amministrazione

A. 1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (artt. 24 e 25 del Decreto)	29
A. 2. AREE A RISCHIO	32
A. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITÀ A RISCHIO	33
A. 4. AREE DI ATTIVITÀ A RISCHIO: ELEMENTI FONDAMENTALI DEL PROCESSO DECISIONALE	36
A. 4.1. Singole operazioni a rischio: individuazione dei Responsabili delle aree a rischio reato e Schede di Evidenza	36
A. 5. COMPITI DELL'ORGANISMO DI VIGILANZA	36

Parte Speciale "B"

Reati Societari

B. 1. LA TIPOLOGIA DEI REATI SOCIETARI (art. 25 ter del Decreto)	39
B. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI	43
B. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	43
B. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI	44
B. 4.1. Bilanci ed altre comunicazioni sociali	45
B. 4.2 . Esercizio dei poteri di controllo sulla gestione sociale	45
B. 4.3. Tutela del capitale sociale	46
B. 5. COMPITI DELL'ORGANISMO DI VIGILANZA	46

Parte Speciale "C"

Delitti informatici e trattamento illecito dei dati

C. 1. LA TIPOLOGIA DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (art. 24bis del Decreto)	49
C. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI	52
C. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	53
C. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI	53
C. 5. COMPITI DELL'ORGANISMO DI VIGILANZA	56

Parte Speciale "D"

Reati in violazione delle norme a tutela della salute e della sicurezza sul luogo di lavoro

D. 1. LA TIPOLOGIA DEI REATI IN VIOLAZIONE DELLE NORME A TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LUOGO DI LAVORO (art. 25 septies del Decreto)	59
D. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI	60
D. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	60
D. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI	62
D. 5. COMPITI DELL'ORGANISMO DI VIGILANZA	64

Parte Speciale "E"

Reati in danno all'amministrazione della giustizia

E. 1. LA TIPOLOGIA DEI REATI IN DANNO ALL'AMMINISTRAZIONE DELLA GIUSTIZIA (art. 25 decies del Decreto)	66
E. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI	66
E. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	66
E. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI	67
E. 5. COMPITI DELL'ORGANISMO DI VIGILANZA	68

Parte Speciale "F"

Delitti in materia di violazione del diritto d'autore

F. 1. LA TIPOLOGIA DEI DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25 novies del Decreto)	70
F. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI	71
F. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	72
F. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI	72
F. 5. COMPITI DELL'ORGANISMO DI VIGILANZA	73

Parte Speciale "G"

Delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

G. 1. LA TIPOLOGIA DEI DELITTI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (art. 25 octies del Decreto)	75
G. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI	76
G. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	76
G. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI	76
G. 5. COMPITI DELL'ORGANISMO DI VIGILANZA	77

ALLEGATI

Parte Generale

- I. Codice Etico
- II. Struttura Organizzativa di Web Consult S.r.l.
- III. Articolazione dei Poteri e Sistema di Deleghe

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMATIVA RILEVANTE

1.1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE.

Il Decreto Legislativo n. 231 dell'8 giugno 2001, che introduce la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (di seguito il "Decreto"), ha adeguato la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali precedentemente sottoscritte dall'Italia, in particolare la *Convenzione di Bruxelles del 26 luglio 1995* sulla tutela degli interessi finanziari della Comunità Europea, la *Convenzione di Bruxelles del 26 maggio 1997* sulla lotta alla corruzione di funzionari pubblici sia della Comunità Europea che degli Stati membri e la *Convenzione OCSE del 17 dicembre 1997* sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il decreto in esame prevede un nuovo tipo di responsabilità che il legislatore denomina "amministrativa", ma che ha forti analogie con la responsabilità penale. Tale responsabilità è molto vicina a quella penale in quanto, non soltanto il suo accertamento avviene nell'ambito del processo penale, ma anche perché essa è autonoma rispetto alla persona fisica che ha commesso il reato: l'ente potrà essere dichiarato responsabile, anche se la persona fisica che ha commesso il reato non è imputabile ovvero non è stata individuata.

I presupposti perché possa incorrere in tale responsabilità sono:

- a) che un soggetto che riveste posizione apicale all'interno della sua struttura, ovvero un sottoposto, abbia commesso uno dei reati previsti dal decreto;
- b) che il reato sia stato commesso nell'interesse o a vantaggio dell'ente¹;
- c) che il reato commesso dalle persone fisiche derivi da una "colpa di organizzazione" dell'ente consistente nel non aver istituito un efficiente ed efficace sistema di controllo interno finalizzato alla prevenzione dei reati.

¹ L'interesse ha una valenza soggettiva, riferita alla volontà dell'autore materiale del reato, mentre il vantaggio ha una valenza di tipo oggettivo riferita ai risultati effettivi della sua condotta. Il legislatore ha voluto rendere punibile l'ente anche nelle ipotesi in cui l'autore del reato, pur non avendo di mira direttamente un interesse dell'ente medesimo, ha realizzato comunque un vantaggio a favore di questo.

Da ciò deriva che non è prefigurabile una responsabilità dell'ente ove la persona fisica che ha commesso il reato abbia agito nell'interesse esclusivo proprio o di terzi ovvero nell'ipotesi in cui all'ente non sia imputabile alcuna "colpa organizzativa".

Quanto alla tipologia di reati cui si applica la disciplina in esame, il legislatore delegato ha inizialmente operato una scelta minimalista rispetto alle indicazioni contenute nella legge delega e, pur evidenziando nella relazione di accompagnamento la prevedibile estensione della disciplina in questione anche ad altre categorie di reati, ne ha inizialmente presi in considerazione soltanto alcuni.

La responsabilità prevista dal Decreto comprende i reati commessi all'estero, purché per gli stessi non proceda lo Stato in cui è stato commesso il reato.

I punti chiave del Decreto riguardano:

a) L'individuazione delle persone che, commettendo un reato nell'interesse o a vantaggio dell'ente, ne possono determinare la responsabilità. In particolare possono essere:

1. persone fisiche che rivestono posizione di vertice ("apicali") (rappresentanza, amministrazione o direzione dell'Ente o di altra unità organizzativa o persone che esercitano, di fatto, la gestione ed il controllo);
2. persone fisiche sottoposte alla direzione o vigilanza da parte di uno dei soggetti sopraindicati.

b) La tipologia dei reati previsti, che riguarda:

- i.* reati commessi in danno della Pubblica Amministrazione;
- ii.* delitti informatici e trattamento illecito di dati;
- iii.* delitti di criminalità organizzata;
- iv.* reati in tema di falsità in monete, carte di pubblico credito e valori in bollo e in strumenti o segni di riconoscimento;
- v.* delitti contro l'industria e il commercio;
- vi.* reati in materia societaria;
- vii.* delitti con finalità di terrorismo o di eversione dell'ordine democratico;
- viii.* pratiche di mutilazione degli organi genitali femminili;
- ix.* delitti contro la personalità individuale, concernenti la riduzione o il mantenimento in schiavitù o in servitù, la tratta di persone e l'acquisto e l'alienazione di schiavi;
- x.* abusi di mercato;
- xi.* reati in violazione delle norme in materia di salute e sicurezza sul lavoro;
- xii.* delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- xiii.* delitti in materia di violazione del diritto d'autore;

xiv. reati in danno all'amministrazione della giustizia;

xv. reati ambientali.

Non tutte le predette categorie di delitti sono tuttavia ad oggi ipotizzate come realizzabili nello svolgimento delle attività tipiche poste in essere da Web Consult S.r.l.. Quelle che possono concretamente considerarsi come rilevanti, in quanto effettivamente realizzabili dai dipendenti e dai collaboratori della società nello svolgimento dell'attività d'impresa, saranno trattate ed esaminate nella Parte Speciale del presente Modello. Nello specifico, stante l'area di attività e la natura di Web Consult S.r.l. si ritiene che dei reati previsti fino ad oggi nel decreto possano potenzialmente riguardare la Società quelli riportati sub *i), ii)vi), x), xi), xii), xiii) e xiv)*. Di questi segue l'elencazione:

Reati in danno della Pubblica Amministrazione:

1. indebita percezione di contributi, finanziamenti o altre erogazioni da parte di un ente pubblico (art. 316-ter c.p.), truffa in danno dello Stato o d'altro ente pubblico (art. 640, 1° comma, n. 1 c.p.);
2. truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
3. frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
4. corruzione per un atto d'ufficio (art. 318 c.p.);
5. corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
6. corruzione in atti giudiziari (art. 319-ter c.p.);
7. induzione indebita a dare o promettere utilità (art. 319-quater c.p.);
8. istigazione alla corruzione (art. 322 c.p.);
9. corruzione di persone incaricate di pubblico servizio (art. 320 c.p.);
10. concussione (art. 317 c.p.);
11. malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.);
12. peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.);
13. turbata libertà degli incanti (art. 353 c.p.).

Reati societari:

1. false comunicazioni sociali (art. 2621 c.c.);
2. fatti di lieve entità (art. 2621 bis c.c.);

3. non punibilità per particolare tenuità (art. 2621 ter c.c.);
4. falso in prospetto (art. 2623 c.c.)²;
5. falsità nelle relazioni o nelle comunicazioni della Società di Revisione (art. 2624 c.c.)³;
6. impedito controllo (art. 2625 c.c.);
7. indebita restituzione dei conferimenti (art. 2626 c.c.);
8. illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
9. illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
10. operazioni in pregiudizio dei creditori (art. 2629 c.c.);
11. formazione fittizia del capitale (art. 2632 c.c.);
12. indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
13. infedeltà patrimoniale (art. 2634 c.c.);
14. illecita influenza sull'assemblea (art. 2636 c.c.);
15. aggio (art. 2637 c.c.);
16. ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.);
17. corruzione tra privati (art. 2635 c.c.).

Reati in violazione delle norme in materia di salute e sicurezza sul lavoro:

1. omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 589 e 590 c.p.).

Delitti informatici e trattamento illecito di dati:

1. falsità in documento informatico (art. 491-bis c.p.);
2. accesso abusivo ad un sistema informatico (art. 615-ter c.p.);
3. detenzione e diffusione abusiva di codici di accesso a sistemi informatici (art. 615-quater c.p.);
4. diffusione di apparecchiature o programmi diretti a danneggiare un sistema informatico (art. 615-quinquies c.p.);
5. cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617 c.p.);

• ² articolo abrogato dall'art. 34 L. 262/2005 con conseguente previsione del delitto di falso in prospetto ai sensi dell'art. 173 bis D.Lgs. 58/1998.

• ³ articolo abrogato dall'art. 37 n. 34 D.Lgs. 39/2010 con conseguente previsione della contravvenzione e del delitto di "falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale" ai sensi dell'art. 27 D.Lgs. 39/2010.

6. installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche (art. 617 bis c.p.);
7. falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617 ter c.p.);
8. intercettazione, impedimento o interruzione illecita di comunicazioni informatiche (art. 617-quater c.p.);
9. installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche (art. 617-quinquies c.p.);
10. Danneggiamento di informazioni, dati e programmi informatici – altrui (art. 635-bis c.p.);
11. Danneggiamento di informazioni, dati e programmi informatici di pubblica utilità (art. 635-ter c.p.);
12. Danneggiamento di sistemi informatici (art. 635-quater c.p.);
13. Danneggiamento di sistemi informatici di pubblica utilità (art. 635-quinquies c.p.);
14. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies).

Delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita:

1. Ricettazione (art. 648 c.p.);
2. Riciclaggio (art. 648-bis c.p.);
3. Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).

Delitti in materia di violazione del diritto d'autore:

1. Mettere a disposizione del pubblico un'opera dell'ingegno protetta (art. 171 c.1 L. 633/1941);
2. Deformare, mutilare, modificare o usurpare la paternità di un'opera altrui non destinata alla pubblicità (art. 171 c.3 lettera a-bis L. 633/1941);
3. Abusiva duplicazione di programmi per elaboratore e rimozione arbitraria o elusione funzionale dei dispositivi di protezione(art. 171-bis c.1 L. 633/1941).

Reati in danno all'amministrazione della giustizia:

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

1.2. SANZIONI

Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono:

- ◆ Sanzioni pecuniarie;
- ◆ Sanzioni interdittive;
- ◆ Confisca;
- ◆ Pubblicazione della sentenza.

In particolare le principali sanzioni interdittive concernono:

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

1.3. AZIONI ESIMENTI DALLA RESPONSABILITÀ AMMINISTRATIVA

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

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

- a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un *modello di organizzazione e di gestione* idoneo a prevenire reati della specie di quello verificatosi (di seguito il "Modello");
- b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato ad un *Organismo di Vigilanza* dell'Ente (di seguito "OdV"), dotato di autonomi poteri di iniziativa e controllo;
- c) le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il suddetto Modello;
- d) non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV.

Per quanto concerne i dipendenti, l'art. 7 prevede l'esonero nel caso in cui l'ente abbia adottato ed efficacemente attuato prima della commissione del reato un modello di organizzazione gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

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

1. individuare le attività nel cui ambito esiste la possibilità che siano commessi reati;

2. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
3. individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
4. prevedere obblighi di informazione nei confronti dell'OdV;
5. introdurre un *sistema disciplinare* interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

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

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

2. LINEE GUIDA DI CONFINDUSTRIA

La predisposizione del presente Modello è ispirata alle *Linee Guida* emanate da Confindustria, approvate definitivamente il 21/07/2014 ed aggiornate al Marzo 2014 (di seguito le "Linee Guida").

Il percorso da queste indicato per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

- ❖ individuazione delle *aree a rischio*, volta a verificare in quali aree/settori aziendali sia possibile la realizzazione dei reati;
- ❖ predisposizione di un sistema di controllo in grado di ridurre i rischi attraverso l'adozione di appositi protocolli. A supporto di ciò soccorre l'insieme coordinato di strutture organizzative, attività e regole operative applicate – su indicazione del vertice apicale – dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno. Le componenti più rilevanti del sistema di controllo preventivo proposto da Confindustria sono:
 - codice etico;
 - sistema organizzativo;
 - procedure manuali ed informatiche;
 - poteri autorizzativi e di firma;
 - sistemi di controllo e gestione;

- comunicazioni al personale e sua formazione.

Il sistema di controllo inoltre deve essere informato ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- ❖ documentazione dei controlli;
- ❖ introduzione di un adeguato sistema sanzionatorio per le violazioni delle norme e delle procedure previste dal modello;
- ❖ individuazione di un OdV;
- ❖ obbligo da parte delle funzioni aziendali, e segnatamente di quelle individuate come maggiormente “a rischio”, di fornire informazioni all’OdV, sia su base strutturata (informativa periodica in attuazione del Modello stesso), sia per segnalare anomalie o atipicità riscontrate nell’ambito delle informazioni disponibili (in questo ultimo caso l’obbligo è esteso a tutti i dipendenti senza seguire linee gerarchiche);
- ❖ possibilità di attuare in seno ai gruppi soluzioni organizzative che accentrino presso l’OdV della capogruppo le risorse operative da dedicare alla vigilanza anche nelle società del gruppo stesso a condizione che:
 - o in ogni controllata sia istituito l’OdV;
 - o sia possibile per l’OdV della controllata avvalersi delle risorse allocate presso l’OdV della capogruppo sulla base di un predefinito rapporto contrattuale;
 - o i dipendenti dell’OdV della capogruppo, nell’effettuazione dei controlli presso le altre società del gruppo, assumano la veste di professionisti esterni che svolgono la loro attività nell’interesse della controllata, riportando direttamente all’OdV di questa ultima, con i vincoli di riservatezza propri del consulente esterno.

Resta inteso che la scelta di non seguire in alcuni punti specifici le Linee Guida non inficia la validità di un Modello. Questo infatti essendo redatto con riferimento alla peculiarità di una società particolare, può discostarsi dalle Linee Guida che per loro natura hanno carattere generale.

3. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE E GESTIONE DA PARTE DI WEB CONSULT S.r.l.

3.1. MOTIVAZIONI DI WEB CONSULT S.r.l. NELL’ADOZIONE DEL MODELLO DI ORGANIZZAZIONE E GESTIONE

Web Consult S.r.l., al fine di assicurare sempre più condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha ritenuto conforme alle proprie politiche aziendali procedere all'adozione di un modello di organizzazione e di gestione in linea con le prescrizioni del Decreto e sulla base delle Linee Guida emanate da Confindustria.

Tale iniziativa, unitamente all'adozione del Codice Etico è stata assunta nella convinzione che l'adozione di tale Modello - al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio - possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti della Società e di tutti gli altri soggetti alla stessa cointeressati (Clienti, Fornitori, Collaboratori a diverso titolo), affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

3.2. FINALITÀ DEL MODELLO

Il Modello predisposto da Web Consult S.r.l. si fonda su procedure ed attività di controllo che nella sostanza:

- ◆ individuano le aree/i processi di possibile rischio nell'attività aziendale vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
- ◆ definiscono un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni della società in relazione ai rischi/reati da prevenire tramite:
 - o un Codice Etico, che fissa le linee di orientamento generali, e procedure formalizzate, tese a disciplinare in dettaglio le modalità operative nei settori "sensibili";
 - o un sistema di deleghe di funzioni e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
- ◆ determinano una struttura organizzativa coerente volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;
- ◆ individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- ◆ attribuiscono all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporre l'aggiornamento.

Pertanto il Modello si propone come finalità quelle di:

- predisporre idonee iniziative di prevenzione e controllo finalizzate alla riduzione del rischio di commissione dei reati connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome e per conto di Web Consult S.r.l. nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di Web Consult S.r.l. che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale.
- ribadire che Web Consult S.r.l. non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarre vantaggio) sono comunque contrari ai principi etici cui Web Consult S.r.l. intende attenersi.

3.3. STRUTTURA DEL DOCUMENTO

Il presente documento (Modello) è costituito da una "Parte Generale" e da singole "Parti Speciali", predisposte per le diverse tipologie di reato contemplate nel Decreto 231/2001 e considerate rilevanti per Web Consult S.r.l. Nella parte generale, dopo un richiamo ai principi del decreto, vengono illustrate le componenti essenziali del modello con particolare riferimento all'OdV, alla formazione del personale ed alla diffusione del modello nel contesto aziendale, al sistema disciplinare e alle misure da adottare in caso di mancata osservanza delle prescrizioni del modello.

La Parte Speciale "A" trova applicazione per le tipologie specifiche di reati previste ai sensi degli articoli 24 e 25 del Decreto, ossia per i reati realizzabili in danno della Pubblica Amministrazione.

La Parte Speciale "B" trova applicazione per le tipologie specifiche di reati previste ai sensi dell'art. 25-ter del Decreto, cioè per i c.d. reati societari.

La parte Speciale "C" trova applicazione per le tipologie specifiche di reati previste ai sensi dell'art. 24-bis del Decreto, cioè per i c.d. Delitti informatici e trattamento illecito dei dati.

La Parte Speciale "D" trova applicazione per le tipologie specifiche di reato previste ai sensi dell'art. 25-septies del Decreto, cioè per i reati in violazione delle norme a tutela della salute e della sicurezza sul luogo di lavoro.

La Parte Speciale “E” trova applicazione per le tipologie specifiche di reato previste ai sensi dell’art. 25-decies del Decreto, cioè per i reati in danno all’amministrazione della giustizia.

La Parte Speciale “F” trova applicazione per le tipologie specifiche di reato previste ai sensi dell’art. 25-novies del Decreto, cioè per i reati in materia di violazione del diritto d’autore.

La parte Speciale “G” trova applicazione per le tipologie specifiche di reato previste ai sensi dell’art. 25-octies del Decreto, cioè per i delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

3.4. MODIFICHE ED INTEGRAZIONI DEL MODELLO

Essendo il presente Modello un “atto di emanazione dell’organo dirigente” (in conformità alle prescrizioni dell’art. 6, comma 1, lettera a del Decreto) la sua adozione, così come le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione di Web Consult S.r.l., fatto salvo quanto diversamente previsto nelle parti speciali del presente Modello.

In particolare è demandato al Consiglio di Amministrazione di Web Consult S.r.l., di integrare il presente Modello con ulteriori Parti Speciali relative ad altre tipologie di reati che, per effetto di nuove normative, possano essere ulteriormente collegate all’ambito di applicazione del Decreto 231.

4. ORGANISMO DI VIGILANZA

4.1. IDENTIFICAZIONE DELL’ORGANISMO DI VIGILANZA

Secondo le disposizioni del Decreto (artt. 6 e 7) e le indicazioni contenute nella Relazione di accompagnamento al Decreto, le caratteristiche dell’OdV debbono essere:

- autonomia e indipendenza;
- professionalità;
- continuità d’azione.

Negli enti di piccole dimensioni i compiti di OdV possono essere svolti direttamente dall’organo dirigente. Secondo le linee guida di Confindustria, in questa sede, la definizione di piccola impresa va ricercata più che in parametri quantitativi nella essenzialità della struttura interna gerarchica e funzionale.

Sulla base di queste considerazioni il Consiglio di Amministrazione di Web Consult S.r.l. ha nominato quale membro dell’ OdV monocratico ai sensi dell’art. 6 commi 1 lettera b e 4 del Decreto:

- l'Avv. Gaetano Picciolo, esperto legale in materia;

Sono pertanto di competenza dell'OdV di Web Consult S.r.l. le attività di vigilanza e controllo previste **dal Modello**.

In considerazione della peculiarità delle proprie attribuzioni e dei contenuti professionali specifici da esse richiesti, l'OdV nello svolgimento dei propri compiti si avvarrà delle prestazioni delle risorse allocate nell'OdV di quelle altre Funzioni che, di volta in volta, si potranno rendere utili allo svolgimento delle attività indicate.

4.2. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA

La *mission* dell'OdV di Web Consult S.r.l. consiste in generale nel:

1. vigilare sull'applicazione del Modello in relazione alle diverse tipologie di reati contemplate dal Decreto;
2. verificare l'efficacia del Modello e la sua capacità di prevenire la commissione dei reati di cui al Decreto;
3. individuare e proporre al Consiglio di amministrazione aggiornamenti e modifiche del Modello stesso in relazione alla mutata normativa o alle mutate condizioni aziendali.

Su di un piano più operativo sono affidati all'OdV di Web Consult S.r.l. i seguenti compiti:

- verificare periodicamente la mappa delle aree a rischio reato al fine di adeguarla ai mutamenti dell'attività e/o della struttura aziendale. A tal fine il Management e gli addetti alle attività di controllo nell'ambito delle singole funzioni devono segnalare all'OdV le eventuali situazioni in grado di esporre l'azienda al rischio di reato. Tutte le comunicazioni devono essere scritte (anche via e-mail) e non anonime;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici, posti in essere nell'ambito delle aree di attività a rischio come definite nelle singole Parti Speciali del Modello;
- raccogliere, elaborare e conservare le informazioni (comprese le segnalazioni di cui al successivo paragrafo 4.4) rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV (v. successivo paragrafo 4.4);
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello portate all'attenzione dell'OdV da segnalazioni o emerse nel corso dell'attività di vigilanza dello stesso;

- verificare che gli elementi previsti dalle singole Parti Speciali del Modello per le diverse tipologie di reati (adozione di clausole standard, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a proporre aggiornamenti degli elementi stessi.

Per lo svolgimento dei compiti suddetti l'OdV:

- gode di ampi poteri ispettivi e di accesso ai documenti aziendali;
- dispone di risorse finanziarie e professionali adeguate;
- si avvale del supporto e la cooperazione delle varie strutture aziendali che possano essere interessate o comunque coinvolte nelle attività di controllo.

4.3. REPORTING DELL'ORGANISMO DI VIGILANZA NEI CONFRONTI DEGLI ORGANI SOCIETARI

L'OdV di Web Consult S.r.l. effettua un reporting periodico nei confronti del Consiglio di Amministrazione.

Ogni anno, inoltre, l'OdV di Web Consult S.r.l. trasmette al Consiglio di Amministrazione, un rapporto scritto sull'attuazione del Modello presso Web Consult S.r.l.

4.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

4.4.1. Segnalazioni da parte di esponenti aziendali o da parte di terzi.

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

Valgono al riguardo le seguenti prescrizioni:

- ◆ devono essere raccolte eventuali segnalazioni relative alla violazione del Modello o comunque conseguenti a comportamenti non in linea con le regole di condotta adottate dalla Società stessa;
- ◆ l'OdV valuterà le segnalazioni ricevute e le eventuali conseguenti iniziative a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto; eventuali rifiuti di procedere ad una indagine interna;
- ◆ le segnalazioni, in linea con quanto previsto dal Codice Etico, dovranno essere in forma scritta e non anonima ed avere ad oggetto ogni violazione o sospetto di violazione del Modello;

- ◆ l'OdV agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede;
- ◆ al fine di facilitare il flusso di segnalazioni ed informazioni verso l'OdV è operativa una casella di posta elettronica odv.webconsult@tecnocasa.com da utilizzare per la segnalazione delle violazioni o anche solo dei sospetti di violazione del Modello;
- ◆ le segnalazioni pervenute all'OdV devono essere raccolte e conservate in un apposito archivio al quale sia consentito l'accesso solo ai membri dell'OdV;

4.4.2. Obblighi di informativa relativi ad atti ufficiali

Oltre alle segnalazioni anche ufficiose di cui al capitolo precedente, devono essere obbligatoriamente trasmesse all'OdV di Web Consult S.r.l. le informative concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai quadri in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello organizzativo con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

4.4.3. Sistema delle deleghe

All'OdV, infine, deve essere comunicato il sistema delle deleghe adottato da Web Consult S.r.l. ed ogni modifica che intervenga sullo stesso.

5. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE

5.1. INTRODUZIONE

La Società, al fine di dare efficace attuazione al Modello adottato, intende assicurare una corretta divulgazione dei contenuti e dei principi dello stesso all'interno e all'esterno della propria struttura.

In particolare, l'obiettivo della Società è di estendere la comunicazione dei contenuti e dei principi del Modello non solo ai propri dipendenti ma anche ai soggetti che, pur non rivestendo la qualifica formale di dipendente, operano anche occasionalmente per il conseguimento degli obiettivi di Web Consult S.r.l. in forza di contratti.

Sebbene tale attività di comunicazione sia diversamente caratterizzata a seconda dei destinatari cui essa si rivolge, l'informazione concernente i contenuti e i principi del Modello sarà, comunque, improntata a completezza, tempestività, accuratezza, accessibilità e continuità, al fine di consentire ai diversi destinatari la piena consapevolezza di quelle disposizioni aziendali che sono tenuti a rispettare.

In tale contesto, la Società provvederà a porre in essere idonee iniziative dirette a far conoscere e diffondere il Modello con tempestività.

5.2. DIFFUSIONE E INFORMAZIONE

I contenuti del Modello saranno portati a conoscenza di tutti i dipendenti, i collaboratori e gli altri soggetti che intrattengano con la Società rapporti di collaborazione contrattualmente regolati, in ossequio al principio della "massima diffusione" interna ed esterna dei valori, dei principi e delle prescrizioni contenuto nel Modello.

Per i dipendenti e i collaboratori dovrà essere garantita la possibilità di accedere e consultare la documentazione costituente il Modello direttamente sulla rete aziendale, mentre per gli altri soggetti destinatari del modello la suddetta documentazione dovrà essere disponibile sul sito web aziendale o comunque trasmessa e/o consegnata direttamente.

Tra gli strumenti di informazione e comunicazione interna potrà essere predisposto un canale tematico e l'indirizzo di posta elettronica **odv.webconsult@tecnocasa.com** a disposizione di tutti i destinatari anche per eventuali segnalazioni all'OdV.

Inoltre, al fine di agevolare la comprensione del Modello, la Società organizzerà, attraverso l'unità organizzativa aziendale preposta alla formazione, idonei percorsi formativi che potranno concretizzarsi, a seconda dei casi, attraverso la distribuzione di prodotti di e-learning e/o in corsi da tenersi in aula. A completamento delle attività di formazione sarà prevista la compilazione di questionari e delle relative dichiarazioni attestanti l'avvenuta formazione. Il piano di formazione sarà concordato nei contenuti e nelle modalità con l'Organismo di Vigilanza.

L'attività di formazione dovrà essere ponderata in modo da prevedere l'approfondimento e la conoscenza del modello in considerazione delle funzioni, dei compiti, e delle mansioni, svolte dai dipendenti e dagli apicali.

La Società provvederà nel corso di tali attività a rendere noto ai dipendenti che gli stessi sono tenuti a conoscere i principi ed i contenuti del Modello ed a contribuire, in relazione al ruolo e alle responsabilità rivestite all'interno di Web Consult S.r.l., alla sua attuazione e al suo rispetto, segnalando eventuali carenze.

Ai componenti degli organi sociali sarà resa disponibile copia cartacea della versione integrale del documento illustrativo del Modello e sarà fatto loro sottoscrivere un impegno di osservanza dei contenuti del Modello stesso.

Per i neo-assunti verrà prevista una apposita clausola nel contratto di lavoro.

Idonei strumenti di comunicazione saranno adottati per aggiornare i destinatari circa le eventuali modifiche apportate al Modello.

5.3. CLAUSOLE CONTRATTUALI

Al fine di favorire il rispetto del Modello da parte di tutti i soggetti che interagiscono a vario titolo con la Società (collaboratori, consulenti, fornitori, outsourcers etc.), quest'ultima provvederà ad inserire nei contratti clausole standard che impegnino a:

- non adottare atti o intrattenere comportamenti tali da determinare una violazione del Modello;
- adempiere ai percorsi formativi previsti dal presente documento.

In caso di violazione di tali obblighi, dovrà essere prevista la risoluzione del contratto con eventuale applicazione di penali.

5.4. ADOZIONE DEL CODICE ETICO E SUA DIFFUSIONE

A conferma dell'importanza attribuita dalla Società ai profili etici, con particolare riferimento ai comportamenti improntati al rigore ed all'integrità, che costituiscono alcuni dei principali valori posti alla base del modello culturale aziendale, Web Consult S.r.l. si è dotata di un specifico Codice Etico.

Tale documento costituisce uno strumento di cultura aziendale, teso ad evitare comportamenti ambigui o scorretti, mediante la chiara individuazione delle principali regole da rispettare e con l'avvertenza che comportamenti difforni potranno essere sanzionati. In particolare, in esso è ribadito il principio che la Società chiede ai propri dipendenti (ma anche a collaboratori e consulenti esterni) un comportamento improntato secondo principi di ferrea onestà.

L'orientamento all'etica - e cioè alla riservatezza, alla lealtà ed all'onestà dei comportamenti verso l'esterno e verso l'interno - rappresenta, infatti uno strumento di grande utilità per affrontare le sfide attuali e future e per offrire un contributo concreto al conseguimento degli obiettivi aziendali, trasformando in vantaggio competitivo ed in migliori relazioni aziendali la conoscenza e l'apprezzamento da parte del mercato, del modo di operare della Società.

Una copia del Codice Etico è trasmessa ai clienti, ai fornitori e agli istituti finanziari di riferimento e a chiunque ne faccia richiesta. Copia aggiornata del Codice Etico è altresì resa disponibile sul sito internet aziendale.

6. SISTEMA DISCIPLINARE E MISURE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO

6.1. PRINCIPI GENERALI

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurare l'effettività del Modello stesso. Al riguardo, infatti, l'articolo 6 comma 2, lettera e) del Decreto prevede che i modelli di organizzazione e gestione devono *“introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello”*. L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte da Web Consult S.r.l. in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del modello stesso possano determinare.

6.2. SANZIONI PER I LAVORATORI DIPENDENTI

6.2.1. Quadri, Impiegati, Operai

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

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

In relazione a quanto sopra il Modello fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente.

Tali categorie descrivono i comportamenti sanzionati, a seconda del rilievo che assumono le singole fattispecie considerate, e le sanzioni in concreto previste per la commissione dei fatti stessi a seconda della loro gravità.

In particolare, in applicazione dei “Criteri di correlazione tra le mancanze dei lavoratori ed i provvedimenti disciplinari” contenuti nel vigente Contratto Collettivo Nazionale dei Lavoratori del Commercio, si prevede che:

1) incorre nei provvedimenti di RICHIAMO VERBALE, AMMONIZIONE SCRITTA, MULTA, SOSPENSIONE DAL LAVORO E DALLA RETRIBUZIONE il lavoratore che:

- violi le procedure interne previste dal presente Modello (ad es. che non osservi le procedure prescritte, ometta di dare comunicazione all’OdV delle informazioni prescritte, ometta di svolgere controlli, ecc.) o adotti, nell’espletamento di attività;

- nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una “non esecuzione degli ordini impartiti dall’azienda sia in forma scritta che verbale” di cui ai suddetti “Criteri di correlazione”.

2) incorre, inoltre, anche nel provvedimento di LICENZIAMENTO CON PREAVVISO, il lavoratore che:

adotti nell’espletamento delle attività nelle aree a rischio un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, dovendosi ravvisare in tale comportamento un “atto tale da far venire meno radicalmente la fiducia dell’azienda nei confronti del lavoratore” di cui ai suddetti “Criteri di correlazione”.

3) incorre, infine, anche nel provvedimento di LICENZIAMENTO SENZA PREAVVISO il lavoratore che:

adotti, nell’espletamento delle attività nelle aree a rischio un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico della società di misure previste dal Decreto, dovendosi ravvisare nel suddetto comportamento, una condotta tale da provocare “all’Azienda grave nocumento morale e/o materiale”, nonché da costituire “delitto a termine di legge” di cui ai suddetti “Criteri di correlazione”.

Il sistema disciplinare viene costantemente monitorato dal OdV.

6.2.2. Dirigenti

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

6.3. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

Nel caso di violazione del Modello da parte di Amministratori di Web Consult S.r.l., l'OdV ne informerà tempestivamente il Consiglio di Amministrazione.

Tenuto conto che gli Amministratori di Web Consult S.r.l. sono nominati dall'Assemblea degli Azionisti della Società, nell'ipotesi in cui sia stato disposto il rinvio a giudizio di Amministratori, presunti autori del reato da cui deriva la responsabilità amministrativa della Società, si procederà a convocazione dell'Assemblea degli Azionisti per deliberare in merito alla revoca del mandato.

6.4. MISURE NEI CONFRONTI DI COLLABORATORI ESTERNI

Ogni comportamento posto in essere dai Collaboratori esterni in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di un reato sanzionato dal Decreto potrà determinare, grazie all'attivazione di opportune clausole, la risoluzione del rapporto contrattuale. L'OdV cura l'elaborazione, l'aggiornamento e l'inserimento nelle lettere di incarico o negli accordi con terzi di tali specifiche clausole contrattuali che prevedranno anche l'eventuale richiesta di risarcimento di danni derivanti alla società dall'applicazione da parte del giudice delle misure previste dal Decreto.

7. CONFERMA APPLICAZIONE E ADEGUATEZZA DEL MODELLO

Il Modello Organizzativo sarà soggetto a due tipologie di verifiche:

(i) attività di monitoraggio sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso) attraverso l'istituzione di un sistema di dichiarazioni periodiche da parte dei destinatari del modello con il quale si conferma che non sono state poste in essere azioni non in linea con il Modello Organizzativo come meglio definito nelle parti speciali;

(ii) attività di controllo delle procedure: annualmente l'effettivo funzionamento del presente Modello sarà verificato con le modalità stabilite dall'OdV. Inoltre, sarà intrapresa una review di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'OdV e dagli altri soggetti interessati, degli eventi considerati rischiosi, della consapevolezza del personale rispetto alle ipotesi di reato previste dal Decreto, con verifiche a campione.

L'esito di tale verifica, con l'evidenziazione delle possibili manchevolezze ed i suggerimenti delle azioni da intraprendere, sarà incluso nel rapporto annuale che l'OdV predisponde per il Consiglio di Amministrazione della Società.

PARTE SPECIALE "A"

Reati in danno della Pubblica Amministrazione

A. 1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 DEL DECRETO)

Preliminare all'analisi dei reati contro la Pubblica Amministrazione è la puntualizzazione delle nozioni di Pubblica Amministrazione, di Pubblico Ufficiale e di Incaricato di Pubblico Servizio.

Per Pubblica Amministrazione si intende l'insieme di enti e soggetti pubblici (Stato, ministeri, regioni, province, comuni, etc.) e talora privati (concessionari, amministrazioni aggiudicatrici, S.p.A. miste, etc.) e tutte le altre figure che svolgono in qualche modo la funzione pubblica, nell'interesse della collettività e quindi nell'interesse pubblico. Oggetto della tutela penale nei reati di seguito riportati è il regolare funzionamento degli Enti Pubblici, il buon andamento generale dell'Amministrazione di cui all'art. 97 della Costituzione ovvero la tutela e l'integrità del patrimonio pubblico.

Per Pubblico Ufficiale, ai sensi dell'art. 357 c.p., si intende chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa, laddove si considera pubblica la funzione amministrativa disciplinata da norme di diritto pubblico.

Si intende Pubblico Ufficiale, che esercita la pubblica funzione legislativa, chiunque a livello nazionale e comunitario partecipi all'attività normativa vera e propria nonché l'attività amministrativa collegata. I soggetti pubblici che esercitano tale funzione sono: il Parlamento, il Governo, le Regioni, le Province, le Istituzioni dell'Unione Europea.

Si intende Pubblico Ufficiale, che esercita la pubblica funzione giudiziaria, chiunque a livello nazionale e comunitario svolga sia attività giuridica sia attività amministrativa collegata. I soggetti pubblici che esercitano tale funzione sono: magistrati, cancellieri, segretari, membri della Corte di Giustizia e della Corte dei Conti comunitarie, funzionari e addetti a svolgere l'attività amministrativa collegata.

Si intende Pubblico Ufficiale, che esercita la funzione amministrativa, chiunque abbia il potere di esercitare il potere deliberativo (ovvero quello di formare e manifestare la volontà della Pubblica Amministrazione), autoritativo (ovvero quello di autorizzare o rilasciare concessioni a Privati) e certificativo (ovvero il potere di rappresentare come certa una determinata situazione) della Pubblica Amministrazione.

Per Incaricati di Pubblico Servizio, ai sensi dell'art. 358 c.p., si intende colui che a qualunque titolo presta un pubblico servizio, intendendosi per tale un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima. Esempi di Incaricati di Pubblico Servizio sono i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati.

Si riporta di seguito una breve descrizione dei reati contemplati negli artt. 24 e 25 del Decreto.

Indebita percezione di contributi, finanziamenti o altre erogazioni da parte di un ente pubblico (art. 316ter c.p.)

Il reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea. In questo caso, contrariamente a quanto visto in merito al reato di cui al successivo art. 316bis, non assume alcun rilievo la destinazione dei finanziamenti pubblici erogati, poiché il reato si consuma al momento del loro - indebito - ottenimento. Va infine evidenziato che tale reato, avendo natura residuale, si configura solo qualora la condotta non integri gli estremi del più grave reato di truffa aggravata ai danni dello Stato (art. 640 bis c.p.).

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

Il reato si configura qualora, utilizzando artifici o raggiri e in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro ente pubblico o dell'Unione Europea. Tale reato può realizzarsi quando, ad esempio, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenerne l'aggiudicazione.

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

Il reato si configura qualora la condotta di truffa sopra descritta abbia ad oggetto finanziamenti pubblici, comunque denominati, erogati dallo Stato, da altri enti pubblici o dall'Unione Europea. Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640ter, comma 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico. In concreto, il reato in esame potrebbe configurarsi qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico della Pubblica Amministrazione al fine di inserire un importo superiore a quello legittimamente ottenuto.

Corruzione (artt. 318-319-320 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio si faccia dare o

promettere, per sé o per altri, denaro o altra utilità per compiere, omettere o ritardare atti del suo ufficio ovvero per compiere atti contrari ai suoi doveri di ufficio. Il reato si configura altresì nel caso in cui l'indebita offerta o promessa sia formulata con riferimento ad atti – conformi o contrari ai doveri d'ufficio – già compiuti dal pubblico agente. Il reato sussiste dunque sia nel caso in cui il pubblico ufficiale, dietro corrispettivo, compia un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia nel caso in cui compia un atto contrario ai suoi doveri (ad esempio: garantire l'illegittima aggiudicazione di una gara). Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio. A norma dell'art. 321 c.p., le pene previste per i pubblici ufficiali e gli incaricati di pubblico servizio si applicano anche ai privati che danno o promettono a questi ultimi denaro o altra utilità.

Corruzione in atti giudiziari (art. 319-ter)

Il reato si configura nel caso in cui taluno offra o prometta ad un pubblico ufficiale o ad un incaricato di un pubblico servizio denaro o altra utilità al fine di favorire o danneggiare una parte in un processo civile, penale o amministrativo. Potrà dunque essere chiamata a rispondere del reato la società che, essendo parte in un procedimento giudiziario, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario) al fine di ottenerne la positiva definizione.

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

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

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

La pena prevista per tale reato si applica a chiunque offra o prometta denaro ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per indurlo a compiere un atto contrario o conforme ai doveri d'ufficio, qualora la promessa o l'offerta non vengano accettate. Parimenti, si sanziona la condotta del pubblico agente che solleciti una promessa o un'offerta da parte di un privato.

Concussione (art. 317 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale, abusando della sua qualità o del suo potere, costringa o induca taluno a dare o promettere indebitamente, a sé o ad altri, denaro o altra utilità.

Il reato in esame presenta profili di rischio contenuti ai fini del D.Lgs. 231/01: trattandosi infatti di un reato proprio di soggetti qualificati, la responsabilità dell'ente potrà ravvisarsi solo nei casi in cui un Dipendente od un Agente della Società, nell'interesse o a vantaggio della stessa, *concorra* nel reato del pubblico ufficiale, che, approfittando della propria posizione, esiga prestazioni non dovute.

Malversazione a danno dello Stato (art. 316-bis c.p.)

Il reato punisce il fatto di chi, avendo ottenuto dallo Stato, da altro ente pubblico o dalla Unione Europea, finanziamenti, comunque denominati, destinati a favorire la realizzazione di opere o attività di pubblico interesse, non li destina agli scopi previsti. Poiché il fatto punito consiste nella mancata destinazione del finanziamento erogato allo scopo previsto, il reato può configurarsi anche con riferimento a finanziamenti ottenuti in passato e che non vengano ora destinati alle finalità per cui erano stati erogati.

Turbata libertà degli incanti (art. 353)

Il reato si configura mediante comportamenti fraudolenti volti a falsare il risultato di una procedura ad evidenza pubblica. Il comportamento può essere tenuto con violenza, minaccia, con doni, promesse, collusione od altri mezzi fraudolenti, impedendo o turbando la gara nei pubblici incanti o nelle licitazioni private per conto di Pubbliche Amministrazioni, ovvero allontanandone gli offerenti.

Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati Esteri (art. 322-bis c.p.)

A completamento dell'esame dei reati previsti dall'art. 24 del decreto (concussione, corruzione, istigazione alla corruzione e corruzione in atti giudiziari), si evidenzia che, a norma dell'art. 322bis c.p., i suddetti reati sussistono anche nell'ipotesi in cui essi riguardino pubblici ufficiali stranieri, ossia coloro che svolgano funzioni analoghe a quelle dei pubblici ufficiali italiani nell'ambito di organismi comunitari, di altri Stati membri dell'Unione Europea, di Stati esteri o organizzazioni pubbliche internazionali.

A. 2. AREE A RISCHIO

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato e tale da comprendere anche la Pubblica Amministrazione di Stati esteri).

Vengono pertanto definite aree a rischio tutte quelle aree aziendali che per lo svolgimento della propria attività intrattengono rapporti con le pubbliche amministrazioni. Tenuto conto, pertanto della molteplicità

dei rapporti che Web Consult S.r.l. intrattiene con le Amministrazioni Pubbliche, sono state individuate le seguenti aree di attività ritenute più specificamente a rischio:

Aree a rischio reato:

1. Area tecnica;
2. Amministrazione.

Eventuali integrazioni operative od organizzative, ivi incluse quelle afferenti la mappatura delle aree a rischio, potranno essere decise dal Presidente del Consiglio di Amministrazione della Società. Le aree a rischio reato così identificate hanno costituito il punto di riferimento nella definizione delle procedure di controllo da implementare ai fini dell'adeguamento dell'attuale sistema di controlli interno. La tipologia e la periodicità delle procedure di controllo implementate sulle diverse aree a rischio reato sono state definite tenendo in considerazione la rilevanza dei singoli punti di contatto con la Pubblica Amministrazione.

A. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITÀ A RISCHIO

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti (“Esponenti Aziendali”) operanti nelle aree di attività a rischio nonché da Collaboratori esterni, come già definiti nella Parte Generale (qui di seguito, tutti definiti i “Destinatari”).

La presente Parte Speciale prevede l'espresso divieto – a carico degli Esponenti Aziendali, in via diretta, ed a carico dei Collaboratori esterni, tramite apposite clausole contrattuali – di:

- 1) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);
- 2) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- 3) porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti (sanciti anche dal Codice etico) è fatto divieto in particolare di:

- a) offrire, promettere ed effettuare elargizioni in denaro a pubblici funzionari;

- b) distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice Etico, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte). I regali offerti – salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- c) accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto b);
- d) riconoscere compensi in favore dei Collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- e) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- f) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- 1) i rapporti nei confronti della P.A. per le suddette aree di attività a rischio devono essere gestiti in modo unitario, procedendo alla nomina di un apposito responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio;
- 2) gli incarichi conferiti ai Collaboratori esterni devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito ed essere sottoscritti conformemente alle deleghe ricevute;
- 3) nessun tipo di pagamento può essere effettuato in natura (baratto);
- 4) i pagamenti in denaro contante devono essere limitati ai soli casi strettamente necessari (anticipi per missioni o trasferte, acquisti urgenti, etc.; vanno in ogni caso rispettati i limiti imposti dalla normativa vigente in materia di pagamenti in contante);
- 5) le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;

- 6) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
- 7) nel caso in cui la comunicazione alla Pubblica Amministrazione sia effettuata attraverso supporti informatici, deve essere sempre identificabile l'identità dell'operatore che immette dati e dichiarazioni e che effettua tale comunicazione;
- 8) in caso di richieste di finanziamenti pubblici ovvero in caso di partecipazione a procedure di gara o di negoziazione diretta con la Pubblica Amministrazione dovrà tenersi evidenza in apposito dossier della documentazione a supporto della formazione della decisioni e di tutto il processo decisionale;
- 9) i costi relativi alle utilità concessi a terzi sono, in fase di budget, separate dalle altre voci di costo e imputati a un conto "omaggi a terzi". Colui che effettua un omaggio occasionale a terzi deve compilare e inoltrare il "Modulo autorizzazione omaggi" (vedere format in Allegato A1) all'ufficio contabile autorizzato dal proprio superiore. Per gli omaggi in occasioni di festività o particolari ricorrenze si potrà procedere senza compilazione preventiva del modulo ma con delibera accentrata dell'organo competente;
- 10) l'addetto alla contabilità registra i costi nell'apposito conto "omaggi a terzi" e aggiorna un riepilogo delle spese aventi questa natura, indicando gli importi, il richiedente, le motivazioni e i nominativi dei beneficiari.

In attuazione ai principi generali di comportamento rappresentati nel presente documento e nel Codice Etico, i rapporti con i soggetti istituzionali e con la Pubblica Amministrazione sono gestiti in modo da garantirne la trasparenza e la tracciabilità e pertanto i Destinatari devono:

- operare nel rispetto dei poteri di rappresentanza e di firma a loro conferiti dalla società per il tramite di procure notarili e in generale nell'ambito del sistema delle deleghe di tempo in tempo vigente;
- fare in modo che agli incontri con Pubblici Ufficiali o con Incaricati di Pubblico Servizio partecipino, quando necessario e per quanto necessario, due rappresentanti della società;
- redigere verbali/note interne relativi al contenuto degli incontro con Pubblici Ufficiali o con Incaricati di Pubblico Servizio, per garantire la tracciabilità di quanto emerso, segnalando all'OdV eventuali irregolarità e procedere ad un'ordinata e diligente archiviazione delle predette note (per gli schemi delle suddette note, si rimanda all'Allegato A2 – Scheda di Evidenza);
- riferire all'OdV ogni proposta diretta o indiretta di benefici ricevuta da Pubblici Ufficiali o da Incaricati di Pubblico Servizio, il cui valore ecceda gli usi e le consuetudini comuni.

A. 4. AREE DI ATTIVITÀ A RISCHIO: ELEMENTI FONDAMENTALI DEL PROCESSO DECISIONALE

A. 4.1. SINGOLE OPERAZIONI A RISCHIO: INDIVIDUAZIONE DEI RESPONSABILI DELLE AREE A RISCHIO REATO E SCHEDE DI EVIDENZA

Occorre dare debita evidenza delle operazioni svolte nelle aree a rischio di cui al precedente paragrafo A.2. A tal fine il Presidente del CdA, gli Amministratori Delegati, i Dirigenti Responsabili delle funzioni all'interno delle quali vengano svolte operazioni a rischio divengono *responsabili* delle aree a rischio reato di ogni singola operazione a rischio da loro direttamente svolta o attuata nell'ambito della funzione a loro facente capo. Detti responsabili:

- divengono i soggetti referenti dell'operazione a rischio;
- sono responsabili in particolare dei rapporti con le P.A., per le attività con esse svolte.

Le attività a rischio debbono essere portate a conoscenza dell'OdV dai suddetti responsabili tramite la compilazione di apposite Schede di evidenza (di seguito le "Schede") da aggiornarsi su base periodica (vedere format in allegato A2) da cui risulti:

- a) le Pubbliche Amministrazioni che hanno competenza sulle procedure oggetto dell'operazione;
- b) la dichiarazione rilasciata dal Responsabile dell'area a rischio reato - per sé e per i sub-responsabili delle aree a rischio reato delegati a svolgere attività che comportano rapporti con la Pubblica Amministrazione - da cui risulti che lo stesso è pienamente a conoscenza degli adempimenti da espletare e degli obblighi da osservare nello svolgimento delle operazioni e che non è incorso in reati considerati dal Decreto;
- c) l'indicazione delle principali iniziative e dei principali adempimenti svolti nell'espletamento delle operazioni.

Sulle operazioni in questione l'OdV potrà predisporre ulteriori controlli dei quali verrà data evidenza scritta.

A. 5. COMPITI DELL'ODV

E' compito dell'OdV:

- a) curare l'emanazione e l'aggiornamento di istruzioni standardizzate relative a:
 - la compilazione omogenea e coerente delle Schede di Evidenza;

- gli atteggiamenti da assumere nell'ambito delle Attività a rischio e, in genere, nei rapporti da tenere nei confronti della P.A.;

Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

b) verificare periodicamente – con il supporto delle altre funzioni competenti – il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/ola qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile dell'area a rischio reato od ai sub responsabili;

c) verificare periodicamente, con il supporto delle altre funzioni competenti, la validità di opportune clausole standard finalizzate:

- all'osservanza da parte dei Collaboratori esterni delle disposizioni del Decreto;

- alla possibilità di Web Consult S.r.l. di porre in essere efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;

- all'attuazione di meccanismi sanzionatori (quali il recesso o la risoluzione dal contratto nei riguardi di Collaboratori esterni) qualora si accertino violazioni delle prescrizioni;

d) indicare al management le eventuali integrazioni ai sistemi di gestione finanziaria già presenti in Web Consult S.r.l., con l'evidenza degli accorgimenti opportuni a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

PARTE SPECIALE "B"

Reati societari

B.1. LA TIPOLOGIA DEI REATI SOCIETARI (ART. 25 TER DEL DECRETO)

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-ter del Decreto aggiornati alla L. 27 maggio 2015, n. 69, a decorrere dal 14 giugno 2015.

a) False comunicazioni sociali (art. 2621 c.c.)

Fuori dai casi previsti dall'art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni.

La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

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

Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942, n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

c) Non punibilità per particolare tenuità (art. 2621-ter c.c.)

Ai fini della non punibilità per particolare tenuità del fatto, di cui all'articolo 131-bis del codice penale, il giudice valuta, in modo prevalente, l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori conseguente ai fatti di cui agli articoli 2621 e 2621-bis

d) Falso in prospetto (art. 2623 c.c.)

Commette il reato chi, nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione

alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche d'acquisto o di scambio, espone false informazioni od occulta dati o notizie in modo tale da indurre in errore i destinatari del prospetto (1° comma) ed è una fattispecie delittuosa nell'eventualità che il danno si verifichi (2° comma).

Si precisa che :

o deve sussistere la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto (dolo generico);

o la condotta deve essere idonea ad indurre in inganno i destinatari del prospetto;

o la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto (dolo specifico).

Il reato è costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta incriminata. Il reato si configura come delitto o contravvenzione a seconda che la condotta abbia o meno causato danni patrimoniali ai destinatari del prospetto.

e) Falsità nelle relazioni o nelle comunicazioni della Società di Revisione (art. 2624 c.c.)

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, concernenti la situazione economica patrimoniale o finanziaria della società al fine di conseguire per sé o per gli altri un ingiusto profitto. La sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni.

Soggetti attivi sono i responsabili della Società di Revisione (reato proprio), ma i componenti degli organi di amministrazione di Web Consult S.r.l. ed i suoi dipendenti possono essere coinvolti a titolo di concorso nel reato. E', infatti, ipotizzabile il concorso eventuale, ai sensi dell'art. 110 c.p., degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato o istigato la condotta illecita del responsabile della Società di Revisione.

f) Impedito controllo (art. 2625 c.c.)

Il reato consiste nell'ostacolare o impedire lo svolgimento delle attività di controllo e/o di revisione - legalmente attribuite ai soci, ad organi sociali o a Società di Revisione - attraverso l'occultamento di documenti od altri idonei artifici. Il reato, imputabile esclusivamente agli amministratori, è punito più gravemente se la condotta ha causato un danno.

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

Il reato si configura allorché si proceda, fuori dai casi di legittima riduzione del capitale sociale, alla restituzione anche simulata dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli.

Soggetti attivi del reato sono gli amministratori della società, ma i soci che beneficiano della restituzione o della liberazione possono concorrere nel reato, ai sensi dell'art. 110 c.p., qualora abbiano svolto un'attività di determinazione o istigazione della condotta illecita degli amministratori.

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

Il reato si configura allorché si proceda alla ripartizione di utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva ovvero alla ripartizione di riserve, anche non costituite con utile, che per legge non possono essere distribuite.

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

Soggetti attivi del reato sono gli amministratori della società, ma i soci che beneficiano della restituzione o della liberazione possono concorrere nel reato, ai sensi dell'art. 110 c.p., qualora abbiano svolto un'attività di determinazione o istigazione della condotta illecita degli amministratori.

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

Il reato si configura allorché si proceda, fuori dai casi previsti dalla legge, all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società o della controllante, così da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

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

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

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

Il reato si realizza attraverso riduzioni di capitale sociale, fusioni con altre società o scissioni attuate in violazione delle disposizioni di legge e che cagionino danno ai creditori (reato di evento). Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

m) Omessa comunicazione del conflitto di interessi

Il reato si configura nelle ipotesi di omessa comunicazione da parte dei soggetti destinatari di eventuali conflitti di interesse o di comunicazione di eventuali parti correlate che possano alterare l'obiettività di giudizio.

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

Il reato si configura allorché si proceda alla formazione o all'aumento in modo fittizio del capitale sociale mediante:

- attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

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

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

Il reato si attua quando con atti simulati o con frode si determina la maggioranza in assemblea, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Il reato può essere commesso da chiunque ("reato comune"), quindi anche da soggetti esterni alla società.

p) Aggiotaggio (art. 2637 c.c.)

La realizzazione del reato avviene attraverso la diffusione di notizie false o attraverso operazioni o artifici che provochino una sensibile alterazione del prezzo di strumenti finanziari, quotati o meno, e/o idonei ad accrescere la fiducia del pubblico o di istituti finanziari nella stabilità patrimoniale.

Anche questo è un reato comune che può essere commesso da chiunque.

q) Ostacolo all'esercizio delle autorità pubbliche di vigilanza (art. 2638 c.c.)

Il reato può realizzarsi attraverso due distinte modalità entrambe finalizzate ad ostacolare l'attività di vigilanza delle autorità pubbliche preposte:

- 1) attraverso comunicazioni alle autorità di vigilanza di fatti, sulla situazione economica, patrimoniale o finanziaria, non corrispondenti al vero, ovvero con l'occultamento, in tutto o in parte, difatti che avrebbero dovuto essere comunicati;
- 2) attraverso il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente, in qualsiasi modo.

In entrambe le modalità descritte i soggetti attivi nella realizzazione del reato sono gli amministratori, i direttori generali, i sindaci e il liquidatori.

r) Corruzione tra privati (art. 2635 c.c.)

Il reato si configura quando gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci, i liquidatori, in seguito alla dazione o alla promessa di denaro o altra utilità per sé o per altri, compiono o omettono atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocimento alla società.

s) Infedeltà patrimoniale (art. 2634 c.c.)

Gli amministratori, i direttori generali e i liquidatori, che, avendo un interesse in conflitto con quello della società, al fine di procurare a sé o ad altri un ingiusto profitto o altro vantaggio, compiono o concorrono a deliberare atti di disposizione dei beni sociali, cagionando intenzionalmente alla società un danno patrimoniale, sono puniti con la reclusione da sei mesi a tre anni.

La stessa pena si applica se il fatto è commesso in relazione a beni posseduti o amministrati dalla società per conto di terzi, cagionando a questi ultimi un danno patrimoniale.

In ogni caso non è ingiusto il profitto della società collegata o del gruppo, se compensato da vantaggi, conseguiti o fondatamente prevedibili, derivanti dal collegamento o dall'appartenenza al gruppo.

Per i delitti previsti dal primo e secondo comma si procede a querela della persona offesa.

B. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI

Le aree di attività considerate più specificatamente a rischio in relazione ai reati societari sono ritenute le seguenti:

1. redazione del bilancio, della relazione sulla gestione e di altre comunicazioni sociali;
2. operazioni societarie che possano incidere sull'integrità del capitale sociale;
3. informative e rapporti con gli organi di informazione e stampa.

La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal Codice Etico adottato da Web Consult S.r.l. alla cui osservanza tutti gli amministratori e dipendenti della Società sono tenuti.

Eventuali integrazioni operative od organizzative, ivi incluse quelle afferenti la mappatura delle aree a rischio, potranno essere decise dal Presidente del CdA e dagli Amministratori Delegati della Società.

B. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Destinatari della presente Parte Speciale “B” sono gli Amministratori, i Sindaci, i Dirigenti ed i loro Dipendenti in linea gerarchica che operino nelle aree di attività a rischio (di seguito i “Destinatari”). Ai Destinatari è fatto espresso obbligo di:

- i. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un’informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- ii. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, al fine di garantire la tutela del patrimonio degli investitori, ponendo la massima attenzione ed accuratezza nell’acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative ai prodotti finanziari ed agli emittenti, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell’emittente e sull’evoluzione della sua attività, nonché sui prodotti finanziari e relativi diritti;
- iii. osservare rigorosamente tutte le norme poste dalla legge a tutela dell’integrità ed effettività del capitale sociale e di agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- iv. assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- v. osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne provochino una sensibile alterazione rispetto alla corrente situazione di mercato;
- vi. effettuare con tempestività correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all’esercizio delle funzioni di vigilanza da queste intraprese;
- vii. tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione;
- viii. astenersi dal dare o promettere di dare o ricevere denaro o altra utilità per sé o per altri a vantaggio della società, rispettando la procedura aziendale in materia di gestione omaggi.

B. 4. PRINCIPI DI ATTUAZIONE DEI COMPORAMENTI DESCRITTI

Di seguito sono descritte le modalità di attuazione dei principi soprarichiamati in relazione alle diverse tipologie di reati societari.

B. 4.3. TUTELA DEL CAPITALE SOCIALE.

Per la prevenzione dei reati di cui alle precedenti lettere da f) a m) tutte le operazioni sul capitale sociale della società, di destinazione di utili e riserve, di acquisto e cessione di partecipazioni o di aziende o loro rami di fusione, scissione e scorporo, nonché tutte le operazioni, anche nell'ambito del gruppo, che possano potenzialmente ledere l'integrità del capitale sociale debbono essere realizzate in base a specifiche procedure aziendali e di gruppo all'uopo predisposte.

Queste debbono prevedere:

- l'assegnazione di responsabilità decisionali ed operative per le operazioni anzidette nonché i meccanismi di coordinamento tra le diverse funzioni aziendali coinvolte;
- l'esplicita approvazione da parte del Consiglio di Amministrazione di Web Consult S.r.l.

B. 5. COMPITI DELL'ORGANISMO DI VIGILANZA.

I compiti dell'OdV sono i seguenti:

- monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati di false comunicazioni sociali;
 - esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari;
- b) per quanto riguarda le altre attività a rischio:
- verifiche periodiche sul rispetto delle procedure interne e delle regole di corporate governance;
 - verifica dell'effettiva tracciabilità delle attività e dei flussi informativi;
 - esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

PARTE SPECIALE "C"

Delitti informatici e trattamento illecito dei dati

C. 1. LA TIPOLOGIA DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (ART. 24-BIS DEL DECRETO)

L'art. 24bis prevede che la Società possa essere sanzionata in relazione ai delitti informatici e trattamento illecito di dati, in particolare per quanto riguarda:

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

L'articolo 615-ter del codice penale punisce chiunque acceda abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo. L'oggetto della tutela penale è la salvaguardia del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. Il delitto di accesso abusivo ad un sistema informatico si perfeziona con la violazione del domicilio informatico, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa.

Per "Sistema Informatico" si intende un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli, in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.

Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617 c. p.)

Chiunque, fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni [c.p.p. 266].

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa [c.p. 120; c.p.p. 336]; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale o di un incaricato di un pubblico servizio nell'esercizio o a causa delle funzioni o del servizio, ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-bis c. p.)

Chiunque, fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato.

Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-ter c. p.)

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma falsamente, in tutto o in parte, il testo di una comunicazione o di una conversazione telegrafica o telefonica ovvero altera o sopprime in tutto o in parte il contenuto di una comunicazione o di una conversazione telegrafica o telefonica vera, anche solo occasionalmente intercettata, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato.

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

L'art 617-quater punisce chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle suddette comunicazioni.

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

L'art. 617-quinquies punisce chiunque, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

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

Salvo che il fatto costituisca più grave reato, l'art. 635-bis punisce chiunque distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

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

Salvo che il fatto costituisca più grave reato, l'art. 635-ter punisce chiunque commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

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

Salvo che il fatto costituisca più grave reato, l'art. 635-quater punisce chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.

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

La pena si applica se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

La pena si applica, inoltre, se dal fatto derivi la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile.

Per sistemi informatici o telematici di pubblica utilità si intendono portali quali ad es. Agenzia delle Entrate, ACI, PRA, ecc.

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

L'art. 615-quater punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.

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

L'art. 615-quinques punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.

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

L'art. 491-bis punisce le falsità previste dal capo III del codice penale riguardanti un documento informatico pubblico o privato avente efficacia probatoria.

Le falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

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

L'art. 640-quinques punisce il soggetto che presti servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

In relazione al reato sopra menzionato, si ritiene doveroso sottolineare che Web Consult S.r.l. non è un ente che presta servizi di certificazione ma utilizza solamente strumenti quali la firma elettronica.

C. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI

Tenuto conto dell'elevato grado di informatizzazione aziendale, si ritiene che le attività sensibili riguardino,

ebbene con differenti livelli di esposizione al rischio, l'intera struttura organizzativa nonché tutti i processi aziendali.

C. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Destinatari della presente Parte Speciale “C” sono gli Amministratori, i Sindaci, i Dirigenti e tutti i dipendenti di Web Consult S.r.l. (di seguito i “Destinatari”). Ai Destinatari è fatto espresso obbligo di:

- i. attenersi alle disposizioni e alle procedure informatiche adottate dalla società;
- ii. utilizzare le risorse informatiche esclusivamente per le finalità corrispondenti alla mansione lavorativa assegnata;
- iii. attenersi scrupolosamente alle direttive interne concernenti l'utilizzo degli strumenti informatici nonché il trattamento dei dati;
- iv. astenersi dal porre in essere atti o comportamenti che siano riconducibili alle condotte di reato come delineate nel precedente punto C.1.

C. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI

I Destinatari nello svolgimento delle proprie attività professionali, devono utilizzare gli strumenti e i servizi informatici o telematici nel pieno rispetto delle vigenti normative nonché delle disposizioni aziendali in materia di trattamento dei dati. La società ha definito delle misure di sicurezza organizzative, fisiche, logiche da adottare affinché siano rispettati gli obblighi in materia di sicurezza previsti dal codice in materia di protezione dei dati personali (D. Lgs. 196/03) e dal relativo disciplinare tecnico in materia di misure minime di sicurezza, cui si rimanda. I destinatari sono tenuti ad osservare le istruzioni fornite dalla società con lettera di incarico al trattamento dei dati.

Di seguito si riportano principi, norme e disposizioni per tutti i Destinatari.

- i. Il Personal Computer affidato al dipendente è uno strumento di lavoro; l'utilizzo non inerente l'attività lavorativa può innescare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza, nonché violare le prescrizioni normative di cui all'art. 617-quinquies c.p. e del D. Lgs. 231/01.
- ii. L'accesso al Personal Computer e alla rete aziendale è protetto dalle credenziali di accesso (ovvero Identificativo Utente e Password) che devono essere custodite con la massima cura e diligenza dall'incaricato e non divulgate ad altri soggetti.

- iii. Per ogni incaricato viene creata una “credenziale d’autorizzazione” che consente l’accesso al Personal Computer e alla rete aziendale attraverso una procedura di autenticazione utente; è vietato l’accesso contemporaneo con le stesse credenziali da più elaboratori.
- iv. In caso di assenza o abbandono momentaneo della propria postazione di lavoro, l’incaricato deve adottare misure atte ad escludere che altri soggetti possano acquisire informazioni o accedere ai dati o alla rete; tali misure, a titolo esemplificativo, possono consistere nell’utilizzo di un sistema di oscuramento (screen sever) dotato di password ovvero nello spegnimento del Personal Computer che si sta utilizzando.
- v. Gli strumenti informatici e telematici messi a disposizione da Web Consult S.r.l. costituiscono strumenti di lavoro da utilizzare esclusivamente per l’esecuzione delle mansioni d’ufficio affidate all’incaricato, e non è pertanto consentito il salvataggio o la consultazione di documenti informatici ed elettronici di natura oltraggiosa e/o discriminatoria.
- vi. La password di accesso alle applicazioni e alle banche dati non deve essere facilmente riconducibile all’incaricato, deve rispondere ai criteri di complessità stabilità dall’Amministratore di Sistema e non deve essere in ogni caso comunicata a terzi o trascritta in foglietti visibili ad altri soggetti.
- vii. I supporti removibili di memorizzazione (chiavette USB, hard disk esterni, dvd, cd, floppy, etc.) devono essere custoditi in modo da evitare l’accesso ad altri soggetti; si consiglia al riguardo di custodirli in contenitore munito di serratura; tali supporti possono essere eliminati solo dopo che i dati contenuti siano stati cancellati e resi non recuperabili, in quanto soggetti esperti potrebbero recuperare i dati memorizzati anche dopo la cancellazione.
- viii. Ciascun incaricato è responsabile della dotazione informatica che gli viene assegnato per l’utilizzo delle proprie mansioni e deve custodirla con diligenza sia durante gli spostamenti sia durante l’utilizzo nel luogo di lavoro.
- ix. Non è consentito l’installazione autonoma di programmi nonché modificare autonomamente le caratteristiche hardware e software sul PC assegnato; non è ammesso l’uso di programmi software diversi da quelli forniti da Web Consult S.r.l.
- x. Nell’utilizzo del Fax occorre prestare particolare attenzione qualora vengano trasmessi documenti contenenti dati sensibili: nello specifico si prescrive di digitare correttamente il numero di telefono, controllare l’esattezza del numero digitato prima dell’invio, attendere la stampa del rapporto di trasmissione verificando la corrispondenza tra il numero di pagine inviate e il numero di pagine da inviare; qualora vengano trasmessi dati relativi lo stato di salute, è opportuno chiamare preventivamente il destinatario per assicurarsi il ricevimento della comunicazione direttamente nelle

mani dello stesso evitando in tal modo che terzi o estranei non autorizzati conoscano il contenuto della documentazione oggetto di comunicazione.

- xi. L'archivio telematico di rete deve contenere esclusivamente informazioni strettamente professionali, che vanno altresì esaminate periodicamente per non creare duplicazioni di documenti e di informazioni.
- xii. È proibito entrare nella Rete aziendale e nei programmi utilizzando le credenziali di accesso di altri utenti, anche con l'esplicito consenso di questi ultimi.
- xiii. L'Amministratore del Sistema potrà in qualunque momento provvedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza dei dati, delle informazioni e delle comunicazioni informatiche.
- xiv. Le password di accesso ai sistemi informatici sono configurate dagli utenti, che hanno la possibilità di provvedere alla sostituzione delle password ogni volta che lo ritengono necessario.
- xv. L'Amministratore del Sistema, se richiesto con una comunicazione interna dall'Amministratore Delegato, può rimuovere qualsiasi password per esigenze operative.
- xvi. Il possesso e la detenzione abusiva e la diffusione dei codici di accesso è delegata alla responsabilità dell'utilizzatore di tali codici: è fatto divieto esercitare qualunque attività di utilizzo di tecniche di appropriazione indebita di password tramite mezzi o comportamenti, ai sensi dell'art. 615-quater c.p.
- xvii. È assolutamente vietato configurare sistemi "smartphone" personali per la lettura dell'account di posta elettronica aziendale (casella postale, rubrica, calendario) senza il consenso preventivo dell'Amministratore del Sistema.
- xviii. La casella di posta, assegnata da Web Consult S.r.l. a ogni singolo utente, è uno strumento di lavoro. Le persone assegnatarie della casella di posta elettronica sono responsabili del corretto utilizzo della stessa.
- xix. È vietato utilizzare le caselle di posta aziendali per l'invio di messaggi personali. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti.
- xx. Qualsiasi file allegato alla posta elettronica può essere potenzialmente pericoloso; la posta elettronica può essere falsificata in ogni sua parte. Un messaggio di posta elettronica potrebbe provenire da un mittente diverso da quello indicato nel campo mittente e contenere allegati potenzialmente pericolosi per la sicurezza delle informazioni. La posta elettronica che arriva da mittente sconosciuto va comunque considerata pericolosa e trattata con cautela. In qualsiasi momento ci potrebbero essere dei messaggi di posta elettronica pericolosi non ancora riconosciuti

come tali dai sistemi antivirus. Tutto ciò premesso, gli utenti devono prestare la massima attenzione e cautela nella gestione degli allegati di posta elettronica.

- xxi. Gli utilizzatori della posta elettronica devono prestare la massima attenzione alle minacce di phishing, metodologia che si avvale di messaggi di posta elettronica o siti Web falsificati allo scopo di rubare l'identità di un utente. Gli autori di tali frodi inviano tali messaggi con lo scopo di indurre il maggior numero di persone a divulgare informazioni riservate: la caratteristica di tali messaggi è l'apparente credibilità, ma un'eventuale risposta potrebbe esporre a rischio l'intero sistema informativo aziendale.
- xxii. I personal computer abilitati alla navigazione internet costituiscono uno strumento aziendale necessario allo svolgimento dell'attività lavorativa di ogni utente. È assolutamente vietata la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa stessa.
- xxiii. È fatto divieto all'utente il download di programmi e software da siti internet.
- xxiv. È vietata la registrazione a siti internet i cui contenuti non siano legati all'attività lavorativa, in particolar modo indicando l'indirizzo di posta elettronica fornito da Web Consult S.r.l.
- xxv. Si ammonisce l'utente a non intercettare, interrompere o impedire le comunicazioni informatiche e/o telematiche, tanto meno a danneggiare informazioni, dati o programmi informatici nonché i sistemi informativi o telematici aziendali e/o di pubblica utilità.
- xxvi. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informativo aziendale mediante virus o altre minacce di intrusioni. Ogni utente è tenuto a controllare il regolare funzionamento della protezione antivirus e a segnalare all'Amministratore di Sistema eventuali anomalie riscontrate.
- xxvii. Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
 - a. Sospendere ogni attività in corso
 - b. Spegner il computer
 - c. Segnalare l'accaduto all'Amministratore di Sistema ed attendere istruzioni dallo stesso.
- xxviii. È obbligatorio attenersi alle disposizioni previste nel Documento Programmatico sulla Sicurezza nonché a quanto indicato sulla lettera di individuazione e nomina di incaricato al trattamento di dati e nel CCNL di riferimento.

C. 5. COMPITI DELL'ORGANISMO DI VIGILANZA.

I compiti dell'OdV in relazione all'osservanza e all'efficacia della presente Parte Speciale "C" sono quelli di carattere generale già previsti da Web Consult S.r.l., considerati i controlli operativi posti in essere dal

fornitore dei servizi ICT. All'Organismo di Vigilanza compete tuttavia una verifica periodica sull'esistenza, sulla validità e sull'adeguatezza delle procedure e della documentazione contrattuale in essere presso la società e sul rispetto delle procedure aziendali.

PARTE SPECIALE "D"

Reati in violazione delle norme a tutela della salute e della sicurezza
sul luogo di lavoro

D. 1. LA TIPOLOGIA DEI REATI IN VIOLAZIONE DELLE NORME A TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LUOGO DI LAVORO (ART. 25-SEPTIES DEL DECRETO)

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-*septies* del Decreto la cui commissione possa comunque comportare un beneficio da parte della Società.

Omicidio colposo (art. 589 c.p.)

Il reato si configura nel caso in cui si cagioni la morte di una persona. Ai fini della integrazione del reato, non è richiesto l'elemento soggettivo del dolo, ovvero la coscienza e la volontà di cagionare l'evento lesivo, ma la mera negligenza, imprudenza o imperizia del soggetto agente, ovvero l'inosservanza, da parte di quest'ultimo di leggi, regolamenti, ordini o discipline (art. 43 cod. pen.).

Lesioni colpose gravi o gravissime (art. 590 c.p.)

Il reato si configura nel caso in cui si cagionino ad una persona lesioni gravi o gravissime.

Le lesioni si considerano gravi nel caso in cui: a) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni; b) il fatto produce l'indebolimento permanente di un senso o di un organo (art. 583, comma 1, cod. pen.).

Le lesioni si considerano gravissime se dal fatto deriva: a) una malattia certamente o probabilmente insanabile; b) la perdita di un senso; c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; d) la deformazione, ovvero lo sfregio permanente del viso (art. 583, comma 2, cod. pen.).

Anche ai fini della configurabilità del reato di lesioni colpose, non è necessario che il soggetto agente abbia agito con coscienza e volontà di cagionare l'evento lesivo, essendo sufficiente la mera negligenza, imprudenza o imperizia dello stesso, ovvero l'inosservanza di leggi, regolamenti, ordini o discipline (art. 43 cod. pen.).

Entrambi i reati sopra richiamati rilevano, ai fini del Decreto, unicamente nel caso in cui sia ascrivibile al soggetto agente, sotto il profilo dell'elemento soggettivo, la c.d. "colpa specifica", consistente nella violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene ed alla salute sul lavoro.

Atteso che, in forza di tale circostanza, assume rilevanza la legislazione prevenzionistica vigente, ai fini della presente sezione è stata considerata, in particolare, la normativa di cui al T.U.S., in attuazione della delega di cui all'art. 1 della L. n. 123/2007.

D. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI

Il rischio della commissione dei delitti di omicidio e lesioni colpose non appare particolarmente rilevante.

Si precisa, infatti, che la Società svolge prevalentemente attività d'ufficio e non attività ad alto rischio di pericolosità per la salute e sicurezza dei lavoratori (es. chimico).

La società è comunque da sempre impegnata nell'assunzione e nell'elaborazione di tutte le misure e di tutti i rimedi per ridurre al minimo tali componenti di rischio.

Ai fini del presente protocollo sono considerate a rischio, e pertanto sensibili, tutte le aree di attività aziendali.

D. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Web Consult S.r.l. è consapevole che un approccio serio alla problematica della tutela della sicurezza del lavoro non possa limitarsi alla considerazione dei soli dipendenti e collaboratori appartenenti all'organizzazione aziendale, ma deve tenere conto e farsi carico anche di tutti gli altri soggetti che interagiscono e cooperano anche solo occasionalmente con essi. Di conseguenza devono ritenersi destinatari della Parte Speciale sez. D, ciascuno per quanto di sua competenza:

- Tutti i dipendenti e i componenti gli organi societari;
- Tutti i soggetti aziendali che ricoprono ruoli attinenti la gestione della sicurezza e la tutela della salute dei lavoratori e dei luoghi di lavoro (Responsabile del Servizio di Prevenzione e Protezione, Medico Competente);
- Prestatori di servizi esterni e lavoratori di società appaltatrici che operino all'interno delle aree aziendali;
- Collaboratori occasionali;
- Visitatori degli uffici e degli stabilimenti.

È fatto espresso divieto a carico dei Destinatari di:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato di cui all'art. 25-septies del Decreto;
- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle indicate al punto D.1;
- Utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione di reati di cui alla presente Parte Speciale sezione D.

Nello svolgimento delle proprie attività e nei limiti dei rispettivi compiti, funzioni e responsabilità, i Destinatari devono rispettare, oltre alle previsioni ed alle prescrizioni del Modello adottato dalla Società:

- i. la normativa vigente in materia di salute e sicurezza sul lavoro;
- ii. il codice etico;
- iii. i manuali e le procedure aziendali vigenti in materia di salute e sicurezza sul lavoro;
- iv. il sistema disciplinare.

In particolare, i Destinatari devono prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti nei luoghi di lavoro, su cui ricadono gli effetti delle loro azioni o omissioni, conformemente alla formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

I Lavoratori devono:

- contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sul lavoro;
- osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
- utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto ed i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
- segnalare immediatamente al datore di lavoro, al dirigente o al preposto eventuali carenze nei mezzi e nei dispositivi di protezione individuale, nonché qualsiasi eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- astenersi dal rimuovere o dal modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;

- provvedere alla cura dei mezzi di protezione individuale messi a loro disposizione, senza apportarvi alcuna modifica di propria iniziativa e segnalando al datore di lavoro o al dirigente o al preposto eventuali difetti o inconvenienti negli stessi;
- astenersi dal compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;
- sottoporsi ai controlli sanitari previsti dalla normativa vigente o comunque disposti dal medico competente.

D. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI

La Società si impegna a garantire il rispetto della normativa in materia di tutela della salute e sicurezza sul lavoro, nonché ad assicurare, in generale, un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività lavorativa, anche attraverso:

- la valutazione dei rischi per la salute e la sicurezza;
- la programmazione dell'attività di prevenzione finalizzata ad integrare in modo coerente le condizioni tecniche produttive dell'azienda, nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;
- l'eliminazione dei rischi ovvero, ove ciò non sia possibile, la loro riduzione al minimo e, quindi, la loro gestione in relazione alle conoscenze acquisite in base al progresso tecnico;
- il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, anche al fine di attenuare il lavoro monotono e quello ripetitivo;
- la riduzione dei rischi alla fonte;
- la sostituzione di ciò che è pericoloso con ciò che non lo è o è meno pericoloso;
- la limitazione al minimo del numero di lavoratori che sono, o che possono essere, esposti a rischi;
- compatibilmente con la tipologia della propria attività di impresa, l'utilizzo limitato di agenti chimici, fisici e biologici sul luogo di lavoro;
- la definizione di adeguate misure di protezione collettiva e individuale, fermo restando che le prime dovranno avere priorità sulle seconde;
- il controllo sanitario dei lavoratori in funzione dei rischi specifici;
- l'allontanamento di un lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e, ove possibile, l'assegnazione ad altra mansione;

- adeguata comunicazione e coinvolgimento dei Destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla salute ed alla sicurezza sul lavoro; in quest'ottica, particolare rilevanza è riconosciuta alla consultazione preventiva dei soggetti interessati in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;
- la formazione e l'addestramento adeguati ai Destinatari, nei limiti dei rispettivi ruoli aziendali, funzioni e responsabilità, relativi alla salute e sicurezza sul lavoro, con fine di assicurare la consapevolezza dell'importanza, della conformità delle azioni, rispetto al Modello e delle possibili conseguenze dovute a comportamenti che si discostino dalle regole dettate dallo stesso;
- erogazione di adeguata e continua formazione dei soggetti che svolgono compiti che possono incidere sulla salute e la sicurezza sul lavoro;
- la formalizzazione di istruzioni adeguate ai lavoratori;
- la definizione di idonee misure igieniche, nonché di adeguate misure di emergenza da attuare in caso di pronto soccorso, di procedure antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;
- l'uso di segnali di avvertimento e sicurezza;
- la regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

Le misure relative alla sicurezza e alla salute durante il lavoro non devono in nessun caso comportare oneri finanziari per i Lavoratori. Nell'ambito specifico della gestione della sicurezza sul lavoro e della tutela dell'igiene e salute sul lavoro, nel rispetto di quanto previsto dal T.U.S., sono previste specifiche procedure, in forza delle quali:

- vengono individuati dal Servizio di Prevenzione e Protezione i rischi in materia di sicurezza e tutela dell'igiene e salute sul lavoro;
- il documento di valutazione dei rischi viene aggiornato periodicamente ed in caso di significative modifiche organizzative;
- il Servizio di Prevenzione e Protezione nella valutazione dei rischi adotta criteri oggettivi, documentati e ripetibili, considerando, per ogni specifico rischio, la probabilità di accadimento, la dimensione dell'impatto del danno possibile, i risultati di rilievi ambientali e l'analisi degli infortuni verificatisi nello svolgimento delle attività lavorative;
- vengono definiti e periodicamente aggiornati il piano di intervento delle azioni di prevenzione e protezione sulla base del risultato della valutazione dei rischi effettuata, nonché i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute;

- il Servizio di Prevenzione e Protezione propone ed elabora adeguate procedure volte alla tutela della sicurezza, dell'igiene e della salute sul lavoro nonché indicazioni sulle adeguate misure di prevenzione e protezione da adottare;
- i dirigenti e i preposti sono tenuti a sorvegliare sull'effettivo rispetto delle procedure proposte ed elaborate dal Servizio di Prevenzione e Protezione e sull'adozione di adeguate misure di prevenzione e protezione e a comunicare tempestivamente al Servizio di Prevenzione e Protezione eventuali eccezioni e criticità per il tramite del Datore di Lavoro;
- relativamente alle emergenze, vengono definiti il metodo di individuazione, gli obblighi di segnalazione e i comportamenti da tenere al verificarsi delle stesse; tali aspetti riguardano sia gli addetti alla gestione delle emergenze sia gli altri soggetti che possono essere coinvolti;
- i lavoratori, sulla base dei rischi cui sono esposti, ricevono adeguata informazione e formazione in merito alle misure di prevenzione e protezione da adottare nello svolgimento delle proprie attività e alla gestione delle emergenze;
- in caso di ispezioni giudiziarie e amministrative (es. relative al T.U.S.) devono partecipare i soggetti a ciò espressamente delegati. L'OdV dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura del responsabile dell'area aziendale interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti appositi verbali, che verranno conservati dall'OdV.

D. 5. COMPITI DELL'ORGANISMO DI VIGILANZA.

L'Organismo di Vigilanza:

- propone che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a Rischio, come individuate nella presente Parte Speciale;
- svolge verifiche periodiche sul rispetto delle procedure interne e valuta periodicamente la loro efficacia a prevenire la commissione dei Reati di omicidio colposo e lesioni gravi o gravissime commesse con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro; a tal fine si avvale del supporto operativo del Responsabile del Servizio di Prevenzione e Protezione;
- esamina eventuali segnalazioni di presunte violazioni del Modello ed effettua gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

PARTE SPECIALE "E"

Reati in danno all'amministrazione della giustizia

E. 1. LA TIPOLOGIA DEI REATI IN DANNO ALL'AMMINISTRAZIONE DELLA GIUSTIZIA (ART. 25-DECIES DEL DECRETO)

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-*decies* del Decreto la cui commissione possa comunque comportare un beneficio da parte della Società.

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

Il reato in esame è stato introdotto nel nostro ordinamento con la legge n. 63 del 2001 sul giusto processo. Soggetto attivo può essere chiunque, mentre il destinatario della condotta può essere soltanto chi ha la facoltà di non rispondere in un processo penale, ossia l'indagato o l'imputato, nell'unico processo oppure in un procedimento connesso.

E. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI

Il reato in oggetto può assumere rilevanza per Web Consult S.r.l. nell'ipotesi in cui possa verificarsi un processo penale a carico di un qualsiasi soggetto della Società, amministratore, consigliere e/o sindaco, responsabile e/o dirigente, dipendente e altro soggetto della Società, imputato nel medesimo procedimento penale o in procedimento connesso, che ponga in essere la condotta descritta nel reato di cui all'art. 377 bis c.p., finalizzata a non far rendere dichiarazioni o a rendere dichiarazioni mendaci nel processo penale.

A titolo di mero esempio, nella ipotesi che vengano indagati l'Amministratore Delegato ed in concorso il Responsabile Amministrativo per reati societari o altri reati commessi nell'ambito della propria attività o ruolo all'interno dell'azienda, il primo, con violenza o minaccia, o con promessa di denaro o altre utilità, induce il secondo a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

In conseguenza del fatto che gli interventi ispettivi e le attività di verifica possono riguardare tutte le attività aziendali, tutte le aree aziendali sono aree sensibili per l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

E. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Destinatari della parte speciale E sono tutti i dipendenti e i collaboratori di Web Consult S.r.l.

Si dispone a tutti i destinatari di fornire la massima collaborazione e trasparenza in caso di coinvolgimento a qualunque titolo in un procedimento penale.

E .4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI

Web Consult S.r.l. persegue una politica di trasparenza nelle relazioni con l'autorità giudiziaria e, più in generale, con ogni autorità che abbia compiti di verifica e controllo inerenti le attività svolte dalla Società. Ne consegue che le disposizioni di cui alla presente sezione sono da ritenersi applicabili non solamente nei confronti degli organi riconducibili all'Autorità Giudiziaria, ivi compresa la Polizia Giudiziaria, ma anche a coloro che rivestono funzioni di controllo da parte della Pubblica Amministrazione o altro Ente (a titolo esemplificativo, Ispettorato del Lavoro, personale INAIL, personale ASL, etc.).

La regola generale è l'informazione e la formazione dei dipendenti sulla centralità dei valori etici e sullo spirito di trasparenza e collaborazione che contraddistingue la Società soprattutto nei rapporti con la Pubblica Amministrazione, ivi compresa l'Autorità Giudiziaria.

In caso di visite ispettive, gli esponenti della pubblica amministrazione sono liberi di porre domande ai dipendenti della società:

- tali colloqui sono riservati e il responsabile di funzione non è tenuto a prenderne parte;
- i colloqui devono avvenire in luoghi idonei e non sorvegliati né tanto meno video sorvegliati;
- è vietato ai soggetti apicali impartire istruzioni, consigliare o suggerire risposte alle domande che si presume vengano rivolte all'intervistato;
- è fatto divieto di ogni pratica di discriminazione conseguente alle dichiarazioni rese dall'intervistato e apprese in qualunque modo;
- ogni ingresso di personale ispettivo deve essere annotato e prontamente comunicato all'OdV con sommaria descrizione dell'attività ispettiva subita, delle persone sentite e delle risultanze emerse e allegando eventuali istruzioni generali di comportamento trasmesse dalla Direzione al personale della società.

Relativamente alla gestione del contenzioso, essa è svolta secondo principi di legalità, correttezza, lealtà e trasparenza. Gli incarichi conferiti a legali esterni sono formalizzati tramite un contratto scritto, nel quale sono indicati l'oggetto e i criteri per la determinazione del prezzo. Detto mandato deve essere integrato con una specifica dichiarazione che regola le conseguenze della violazione delle norme di cui al Decreto, con particolare riferimento alle disposizioni in materia di corruzione in atti giudiziari e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

Lo svolgimento della prestazione da parte del legale esterno deve sempre avvenire con la massima trasparenza e questi deve informare periodicamente la Società in ordine alle attività svolte.

E. 5. COMPITI DELL'ORGANISMO DI VIGILANZA.

L'Organismo di Vigilanza riceve la comunicazione relativa alla visita ispettiva di cui al precedente paragrafo E. 4. e, se ritiene che le modalità di gestione dell'ingresso del personale ispettivo siano state condotte con violazione alle disposizioni contenute nella presente Parte Speciale E, informa prontamente l'Organo Amministrativo.

L'Organismo Di Vigilanza è libero di agire in qualunque altro modo ritenga opportuno per verificare il rispetto della veridicità nelle informazioni ed in qualsivoglia comunicazione da rendere all'Autorità e, in caso di constatate violazioni, relaziona l'Organo amministrativo l'accaduto per gli opportuni provvedimenti, indicando le possibili procedure idonee a prevenire, nel futuro, analoghe violazioni.

Qualora la violazione sia da attribuirsi all'Organo amministrativo, l'ODV riferisce all'Assemblea l'accaduto, per i provvedimenti da adottarsi.

PARTE SPECIALE "F"

Delitti in materia di violazione del diritto d'autore

F. 1. LA TIPOLOGIA DEI DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES DEL DECRETO)

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-*novies* del Decreto che si ritengono applicabili all'attività svolta da Web Consult S.r.l. la cui commissione possa comunque comportare un beneficio da parte della Società.

Art. 171

Salvo quanto previsto dall'[art. 171-bis](#) e dall'[articolo 171-ter](#) è punito con la multa da euro 51 (lire 100.000) a euro 2.065 (lire 4 milioni) chiunque senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana;

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;

[e) riproduce con qualsiasi processo di duplicazione dischi o altri apparecchi analoghi o li smercia, ovvero introduce nel territorio dello Stato le riproduzioni così fatte all'estero;]

f) in violazione dell'[art. 79](#) ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma

corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 (lire 1.000.000), se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicità ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

La violazione delle disposizioni di cui al terzo ed al quarto comma dell'[articolo 68](#) comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da euro 1.032 a euro 5.164 (due a dieci milioni di lire).

Art. 171-bis

1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 (lire cinque milioni) a euro 15.493 (lire trenta milioni). La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 (lire trenta milioni) se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli [articoli 64-quinquies](#) e [64-sexies](#), ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli [articoli 102-bis](#) e [102-ter](#), ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 (lire cinque milioni) a euro 15.493 (lire trenta milioni). La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 (lire trenta milioni) se il fatto è di rilevante gravità.

F. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI

Il reato di messa a disposizione del pubblico di un'opera dell'ingegno protetta e usurpazione della paternità di un'opera può assumere rilevanza, sebbene con bassa probabilità di commissione, per Web Consult S.r.l. nelle attività di Progettazione mentre il reato di abusiva duplicazione di programmi per un elaboratore presenta un rischio maggiore in quanto può essere commesso da tutti i dipendenti muniti di PC aziendale.

F. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Destinatari della parte speciale F sono tutti i dipendenti e i collaboratori di Web Consult S.r.l.

Si dispone a tutti i destinatari di:

- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti che integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- attenersi ai principi e alle procedure aziendali di tempo in tempo adottati dalla Società;
- tenere un comportamento corretto, trasparente e conforme alla normativa aziendale interna in tutte le attività aziendali che comportano l'utilizzo di sistemi e apparecchiature informatiche.

F. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI

Si rimanda alle disposizioni previste nella Parte Speciale “C”, e nello specifico si richiama i Destinatari al rispetto delle norme di comportamento di seguito elencate. È fatto divieto di:

- installare programmi software diversi da quelli messi a disposizione dalla società;
- scaricare da Internet programmi senza la preventiva autorizzazione;
- acquistare licenza software da una fonte non certificata che non fornisce idonee garanzie in merito all'originalità/autenticità del software;
- detenere supporti di memorizzazione (DVD, CD, floppy disk, supporti di memorizzazione removibili) di programmi non originali;
- installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza acquistata;
- utilizzare password di computer, codici di accesso o informazioni simili per accedere a programmi, software, banche dati non autorizzati dalla società e comunque estranei alle proprie mansioni lavorative;
- utilizzare strumenti, apparecchiature, programmi informatici, per decriptare software o altri dati informatici;

- distribuire software aziendali a soggetti terzi;
- realizzare codici software che violano copyright di terzi;
- accedere illegalmente a banche dati e duplicare o riprodurre contenuti;
- mettere a disposizione del pubblico un'opera di ingegno protetta e porre in essere comportamenti atti a usurpare la paternità di un'opera.

F. 5. COMPITI DELL'ORGANISMO DI VIGILANZA

I compiti dell'OdV in relazione all'osservanza e all'efficacia della presente Parte Speciale "F" sono quelli di carattere generale già previsti da Web Consult S.r.l., considerati i controlli operativi posti in essere dal fornitore dei servizi ICT.

I controlli a cura dell'amministratore di sistema sono finalizzati a verificare:

- l'analisi dei contratti di licenza stipulati dalla società e la verifica della corrispondenza tra il numero di copie concesse in licenza di uno specifico software con il numero di copie effettivamente installato sui computer presenti in azienda;
- le garanzie rilasciate dai fornitori o dai rivenditori di software in merito all'originalità/autenticità del software;
- i software installati sui computer e sui dispositivi presenti in azienda;
- l'originalità dei supporti di memorizzazione presenti in azienda, controllando l'effettiva presenza del c.d. bollino SIAE;
- che non siano utilizzati o distribuiti all'interno o all'esterno della società, product key per programmi senza la necessaria autorizzazione da parte della funzione aziendale;
- attività di sensibilizzazione nei confronti dei dipendenti sui reati collegati alla c.d. pirateria informatica.

PARTE SPECIALE "G"

Delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

G. 1. LA TIPOLOGIA DEI DELITTI DI RICETTAZIONE, RICICLAGGIO, E IMPIEGO DI DENARO BENI O UTILITA' DI PROVENIENZA ILLECITA (ART. 25-OCTIES DEL DECRETO)

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-*octies* del Decreto che si ritengono applicabili all'attività svolta da Web Consult S.r.l. la cui commissione possa comunque comportare un beneficio da parte della Società.

c.p. art. 648. Ricettazione.

Fuori dei casi di concorso nel reato [\[c.p. 110\]](#), chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329 [\[c.p. 29, 32, 709, 712\]](#). La pena è aumentata quando il fatto riguarda denaro o cose provenienti da delitti di rapina aggravata ai sensi [dell'articolo 628](#), terzo comma, di estorsione aggravata ai sensi [dell'articolo 629](#), secondo comma, ovvero di furto aggravato ai sensi [dell'articolo 625](#), primo comma, n. 7-bis).

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

Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile [\[c.p. 85, 88, 91, 93, 96, 97\]](#) o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto [\[c.p. 45, 46, 47, 49, 50, 649\]](#).

c.p. art. 648-bis. Riciclaggio.

Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000.

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

La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma [dell'articolo 648 \[c.p. 648-quater\]](#).

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

Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli [articoli 648 e 648-bis](#), impiega in

attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000.

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

La pena è diminuita nell'ipotesi di cui al secondo comma [dell'articolo 648](#).

Si applica l'ultimo comma [dell'articolo 648](#) [\[c.p. 648-quater\]](#).

G. 2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI

Le attività aziendali più esposte al rischio di compiere reati di ricettazione, riciclaggio e impiego di proventi illeciti sono:

- ciclo passivo
- ciclo attivo

e pertanto le Aree Sensibili sono:

- Amministrazione e finanza
- Area commerciale.

G. 3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

Destinatari della parte speciale G sono tutti i dipendenti e i collaboratori di Web Consult S.r.l.

In linea generale occorre che tutti i Destinatari:

- tengano un comportamento corretto e trasparente, nel rispetto della normativa interna ed esterna di riferimento;
- si astengano da porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 25-octies del D. Lgs. 231/01;
- si astengano dall'utilizzare anche solo occasionalmente la società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei reati in esame;
- rispettino le disposizioni contenute nel Codice Etico.

G. 4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI

È fatto obbligo a tutti i destinatari del presente Modello di attenersi alle disposizioni di seguito riportate:

- nelle operazioni che possono presentare carattere anomalo per tipologia o oggetto, verificare l'attendibilità commerciale e professionale dei Fornitori, collaboratori esterni e partners

commerciali/finanziari sulla base di alcuni indici rilevanti: dati pregiudizievoli pubblici (bollettino protesti, procedure concorsuali); acquisizione di informazioni commerciali sull'azienda, sui soci e sugli amministratori e sul loro settore di attività; entità del prezzo della transazione e raffronto dello stesso al prezzo normale di mercato; coinvolgimento di “persone politicamente esposte” come definite dal D. Lgs. 231/2007 (ovvero persone fisiche cittadini di altri stati comunitari o di stati extracomunitari che occupano o che hanno occupato importanti cariche pubbliche come pure i loro familiari diretti o coloro con i quali tali persone intrattengono notoriamente stretti legami”;

- verificare la regolarità dei pagamenti, con riferimento alla corrispondenza tra i destinatari/ordinanti dei pagamenti e le controparti effettivamente coinvolte nelle transazioni commerciali;
- controllare i flussi finanziari aziendali, tenendo conto della sede legale della società controparte (paradisi fiscali, paesi a rischio terrorismo), degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e istituti che non hanno insediamenti fisici in alcun paese) e di eventuali schermi societari utilizzati per transazioni o operazioni straordinarie;
- verificare il rispetto delle soglie previste dal D. Lgs. 231/2007 per l'utilizzo di denaro contante o equivalente;
- utilizzare rigorosi criteri di selezione, stipulazione ed esecuzione di accordi/joint-venture con altre imprese per la realizzazione di investimenti;
- verificare la congruità economica di eventuali investimenti effettuati in joint-venture o associazioni temporanee di imprese.

Si precisa inoltre che:

- ai soggetti che effettuano operazioni di natura finanziaria o societaria per conto della Società deve essere formalmente conferito specifico potere con apposita delega per i dipendenti e gli organi sociali ovvero nel relativo contratto di consulenza o di partnership per gli altri soggetti;
- tutti i flussi finanziari sono regolati esclusivamente attraverso canale bancario; i pagamenti in contanti devono essere limitati di numero e di importo unitario esiguo e devono essere adeguatamente monitorati; nessun tipo di pagamento può essere effettuato in natura;
- è fatto divieto di emettere assegni bancari e postali per importi pari o superiori a 1.000 euro, o comunque alla diversa soglia di tempo in tempo stabilita dalla legge, qualora non siano indicati nome o ragione sociale del beneficiario nonché la clausola di non trasferibilità.

G. 5. COMPITI DELL'ORGANISMO DI VIGILANZA

Compiti dell'Organismo di Vigilanza in relazione all'osservanza della presente Parte Speciale G sono quelli di seguito elencati:

- verificare l’emanazione e l’aggiornamento da parte della Società di istruzioni standardizzate relative alle procedure da tenere nelle attività a rischio reato;
- verificare periodicamente il rispetto del sistema delle deleghe in vigore, segnalando eventuali incongruenze e raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile interno;
- verificare il rispetto delle procedure aziendali con particolare riferimento alle attività sensibili;
- verificare periodicamente l’idoneità delle procedure aziendali a mitigare la commissione di rischi reato, segnalando agli organi aziendali le opportune integrazioni ai sistemi gestionali delle risorse finanziarie e alle procedure finalizzate a rilevare in maniera più compiuta l’esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

ALLEGATO I

Codice Etico di Web Consult S.r.l.

CODICE ETICO

*Testo approvato dal Consiglio di Amministrazione
di Web Consult S.r.l. 29/03/2016*

INDICE:

<i>1. PREMESSA</i>	<i>4</i>
<i>1.1. L'Azienda ed il Gruppo</i>	<i>4</i>
<i>1.2. Rapporti con gli stakeholders</i>	<i>4</i>
<i>1.3. I principi di riferimento</i>	<i>4</i>
<i>1.4. Il Codice etico</i>	<i>4</i>
<i>1.5. Ambito di applicazione e destinatari</i>	<i>2</i>
<i>2. PRINCIPI GENERALI</i>	<i>5</i>
<i>2.1 Conformità a leggi e regolamenti</i>	<i>5</i>
<i>2.2 Modelli e regole di comportamento</i>	<i>5</i>
<i>2.3 Riservatezza</i>	<i>6</i>
<i>2.4 Sicurezza sul lavoro</i>	<i>6</i>
<i>2.5 Tutela dell'ambiente</i>	<i>7</i>
<i>2.6 Diffusione ed osservanza del Codice etico</i>	<i>7</i>
<i>2.7 Corporate Governance</i>	<i>7</i>
<i>3. RISORSE UMANE E POLITICA DELL'OCCUPAZIONE</i>	<i>7</i>
<i>3.1 Le condizioni determinanti</i>	<i>7</i>
<i>3.2 Le politiche di selezione</i>	<i>7</i>
<i>3.3 Lo sviluppo delle professionalità</i>	<i>8</i>
<i>3.4 Risorse umane e Codice Etico</i>	<i>8</i>
<i>3.5 Ambiente di lavoro e tutela della privacy</i>	<i>8</i>
<i>4. CONFLITTO DI INTERESSI</i>	<i>8</i>
<i>4.1 Interessi Aziendali ed individuali</i>	<i>8</i>
<i>4.2 Prevenzione dei conflitti di interesse</i>	<i>9</i>
<i>5. PROCEDURE OPERATIVE E DATI CONTABILI</i>	<i>9</i>
<i>5.1 I protocolli specifici</i>	<i>9</i>
<i>5.2 Osservanza delle procedure</i>	<i>9</i>
<i>5.3 Trasparenza contabile</i>	<i>10</i>
<i>6. TUTELA DEL PATRIMONIO SOCIALE</i>	<i>10</i>
<i>6.1 Custodia e gestione delle risorse</i>	<i>10</i>

<i>.2 Operazioni illecite sulle azioni o sul capitale</i>	10
7. RAPPORTI INTERGRUPPO	11
7.1 <i>Autonomia e valori etici comuni</i>	11
7.2 <i>Cooperazione e comunicazione intragruppo</i>	11
8. ORGANISMO DI VIGILANZA	11
8.1 <i>Attribuzioni e caratteristiche</i>	11
8.2 <i>Segnalazioni all'Organismo di Vigilanza</i>	11
9. RAPPORTI CON L'ESTERNO	12
9.1 RAPPORTI CON AUTORITA' ED ISTITUZIONI PUBBLICHE ED ALTRI SOGGETTI RAPPRESENTATIVI DI INTERESSI COLLETTIVI	12
9.1.1 <i>Rapporti con Autorità e Pubbliche Amministrazioni</i>	12
9.1.2 <i>Rapporti con organizzazioni politiche e sindacali</i>	12
9.1.3 <i>Regali, benefici e promesse di favori</i>	12
9.2 RAPPORTI CON CLIENTI E FORNITORI	13
9.2.1 <i>Condotta negli affari</i>	13
9.2.2 <i>Regali, dazioni e benefici</i>	13
10. INFORMATIVA SOCIETARIA	13
10.1 <i>Disponibilità ed accesso alle informazioni</i>	13
10.2 <i>Comunicazioni rilevanti e sollecitazione del mercato</i>	13
11. RAPPORTI CON I MASS MEDIA E GESTIONE DELLE INFORMAZIONI	14
11.1 <i>Modalità di condotta</i>	14
11.2 <i>Informazioni "price sensitive"</i>	14
12. VIOLAZIONI DEL CODICE ETICO – SISTEMA SANZIONATORIO	15
12.1 <i>Segnalazioni delle violazioni</i>	15
12.2 <i>Linee guida del sistema sanzionatorio</i>	15
12.3 <i>Misure nei confronti dei lavoratori subordinati cui si applicano i contratti collettivi (CCNL) per il settore</i>	15
12.4 <i>Misure nei confronti dell'Organo Amministrativo ed Alta Direzione</i>	15
12.5 <i>Misure nei confronti di consulenti e fornitori</i>	15

1. PREMESSA

1.1. L'Azienda ed il Gruppo

Questo Codice (qui di seguito indicato come “Codice Etico”) esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali assunti dai collaboratori di Web Consult S.r.l. (di seguito “la Società”), siano essi dipendenti, collaboratori a vario titolo o amministratori.

La Società fa parte del Gruppo Tecnocasa che, per le dimensioni e l'importanza delle attività, svolge un ruolo rilevante rispetto al mercato dei settori nei quali opera.

Il raggiungimento degli obiettivi della Società è perseguito, da parte di tutti coloro che vi operano, con lealtà, serietà, onestà, competenza e trasparenza, nell'assoluto rispetto delle leggi e delle normative vigenti.

1.2. Rapporti con gli stakeholders

La presenza della Società, l'operatività nei diversi contesti e la molteplicità dei propri interlocutori rende di primaria importanza la gestione dei rapporti tra la Società e gli stakeholders, intendendosi per tali tutti i soggetti pubblici o privati, italiani e stranieri – individui, gruppi, aziende, istituzioni – i cui interessi sono influenzati dagli effetti diretti e indiretti delle attività poste in essere da Web Consult S.r.l. La Società impronta il proprio operato alla puntuale osservanza delle leggi (italiane e dei Paesi in cui la Società è attiva), delle regole di mercato e dei principi ispiratori della concorrenza leale.

1.3. I principi di riferimento

Conformità alle leggi, trasparenza e correttezza gestionale, fiducia e cooperazione con gli stakeholders sono i principi etici cui la Società si ispira – e da cui deriva i propri modelli di condotta - al fine di competere efficacemente e lealmente sul mercato, migliorare la soddisfazione dei propri clienti, accrescere il valore per gli azionisti e sviluppare le competenze e la crescita professionale delle proprie risorse umane. In particolare, la convinzione di agire a vantaggio dell'Azienda non giustifica l'adozione di comportamenti in contrasto con i suddetti principi. Tutti coloro che operano nella Società, senza distinzioni ed eccezioni, sono, pertanto, impegnati ad osservare e far osservare questi principi nell'ambito delle proprie funzioni e responsabilità. Tale impegno si giustifica e richiede che anche i soggetti con i quali ha rapporti a qualunque titolo agiscano nei suoi confronti con regole e modalità ispirate agli stessi valori.

1.4. Il Codice etico

La Società ha ritenuto opportuno e necessario adottare ed emanare un codice di comportamento che esplicita i valori a cui tutti i propri amministratori, dipendenti e collaboratori a vario titolo devono adeguarsi, accettando responsabilità, assetti, ruoli e regole della cui violazione, anche se da essa non consegue alcuna responsabilità aziendale verso terzi, essi assumono la personale responsabilità verso l'interno e verso l'esterno dell'Azienda. La conoscenza e l'osservanza del codice di comportamento da parte di tutti coloro che prestano attività lavorativa a favore della Società sono dunque condizioni primarie per la trasparenza e la reputazione dell'Azienda. Inoltre il codice è portato a conoscenza di tutti coloro con i quali la Società intrattiene rapporti d'affari.

Nell'ambito del sistema dei controlli interni, il Codice Etico costituisce presupposto e riferimento -previa valutazione dei rischi-reato eventualmente connessi alle attività svolte - sia del modello preventivo di

organizzazione gestione e controllo, sia del sistema sanzionatorio per la violazione delle norme in esso stabilite, adottati dalla Società secondo quanto previsto dagli artt. 6 e 7 del D.Lgs. N. 231 del 2001 e sulla base del codice di comportamento redatto da Confindustria ai sensi dell'art. 6, comma 3, del citato decreto legislativo. La vigilanza dell'attuazione del Codice Etico e della sua applicazione è compito di tutti gli amministratori, dirigenti e dipendenti della Società che ne segnalano le eventuali inadempienze o mancata applicazione alle funzioni designate in apposito Ordine di Servizio. La verifica sulla attuazione del codice di comportamento e sulla sua applicazione è di competenza del Consiglio di Amministrazione e del management aziendale, il quale potrà anche farsi promotore di proposte di integrazione o modifica dei contenuti.

E' compito del Consiglio di Amministrazione aggiornare il Codice Etico al fine di adeguarlo alla eventuale nuova normativa rilevante ed alla evoluzione della sensibilità civile. Per quanto riguarda in particolare i reati previsti dal D.Lgs. 231/01 e successive modificazioni, è stato istituito un Organismo di Vigilanza che verifica il funzionamento e l'efficacia del Modello di Organizzazione e gestione adottato dalla Società per la prevenzione dei suddetti reati.

1.5. Ambito di applicazione e destinatari

I principi e le disposizioni del presente Codice sono da ritenersi vincolanti per l'Organo Amministrativo, per i soggetti legati a Web Consult S.r.l. da un rapporto di lavoro subordinato (di seguito anche "dipendenti") e tutti coloro che, a qualsiasi titolo collaborano con la Società (a titolo esemplificativo e non esaustivo: consulenti, agenti, intermediari, lavoratori a progetto, di seguito collettivamente denominati i "collaboratori").

Inoltre Web Consult S.r.l. si impegna a richiedere a tutti i soggetti esterni che interagiscono con la Società (quali partner, clienti e fornitori) il mantenimento di una condotta in linea con i principi generali del presente Codice nonché del Modello di Organizzazione e Gestione adottato dalla Società ai sensi del D. Lgs. 231/01. A tali fine la società si impegna a diffonderne il contenuto e a promuoverne la conoscenza secondo gli strumenti e le modalità di comunicazione ritenute più congrue.

2. PRINCIPI GENERALI

2.1. Conformità a leggi e regolamenti

La Società opera nell'assoluto rispetto delle leggi e delle normative vigenti nei paesi in cui svolge la propria attività, in conformità ai principi fissati nel Codice Etico ed alle procedure previste dai protocolli interni. L'integrità morale è un dovere costante di tutti coloro che lavorano per la Società e caratterizza i comportamenti di tutta la propria organizzazione.

Gli amministratori ed i dipendenti della Società, nonché coloro che a vario titolo operano con la stessa, sono pertanto tenuti, nell'ambito delle rispettive competenze, a conoscere ed osservare le leggi ed i regolamenti vigenti in tutti i Paesi in cui la medesima opera. In tale contesto rientra anche l'attenzione ed il rispetto delle normative che regolano la concorrenza, sia sul mercato nazionale che a livello internazionale. I rapporti con le Autorità di quanti operano per la Società devono essere improntati alla massima correttezza, trasparenza e collaborazione, nel pieno rispetto delle leggi, delle normative e delle loro funzioni istituzionali.

2.2. Modelli e regole di comportamento

Tutte le attività lavorative di quanti operano per la Società devono essere svolte con impegno professionale, rigore morale e correttezza gestionale, anche al fine di tutelare l'immagine dell'Azienda.

I comportamenti ed i rapporti di tutti coloro che a vario titolo operano nell'interesse della Società all'interno ed all'esterno della stessa, devono essere ispirati a trasparenza, correttezza e reciproco rispetto. In tale contesto i dirigenti devono per primi rappresentare con il loro operato un esempio per tutte le risorse umane della Società, attenendosi, nello svolgimento delle proprie funzioni, ai principi ispiratori del Codice Etico, alle procedure ed ai regolamenti aziendali, curandone la diffusione tra i dipendenti e sollecitandoli a presentare richieste di chiarimenti o proposte di aggiornamento ove necessario e verificandone puntualmente la sua applicazione.

Con particolare riferimento agli amministratori, inoltre, la Società si aspetta che questi si adoperino attivamente al fine di proporre e realizzare i progetti, gli investimenti e le azioni industriali, commerciali e gestionali utili a conservare ed accrescere il patrimonio economico, tecnologico e professionale dell'Azienda.

La Società garantisce altresì, sui fenomeni e sulle scelte aziendali, la disponibilità di un supporto informativo tale da consentire alle funzioni ed agli organi societari, agli enti di revisione contabile e di controllo interno, nonché alle autorità di vigilanza, di svolgere la più ampia ed efficace attività di controllo. Tutte le azioni e le relazioni con gli stakeholders nonché quelle intercorrenti tra i destinatari del presente Codice ed i soggetti terzi dovranno essere effettuate garantendo correttezza, completezza, accuratezza, uniformità e tempestività dell'informazione, onde porre gli interessati nella condizioni di prendere decisioni autonome e consapevoli.

Web Consult S.r.l. si impegna ad evitare nelle relazioni, sia interne che esterne, qualsiasi forma di discriminazione basata su età, sesso, orientamento sessuale, stato di salute, razza, nazionalità, opinioni politiche e sindacali nonché fede religiosa.

2.3. Riservatezza

Web Consult S.r.l. assicura il rispetto della riservatezza e la tutela della privacy, anche nel rispetto delle disposizioni contenute del Testo Unico in materia di trattamento dei dati personali (D. Lgs. 196/03) con particolare riferimento alle informazioni acquisite e/o elaborate nello svolgimento della propria attività. La società si astiene dal raccogliere dati riservati salvo in caso di preventiva, espressa e consapevole autorizzazione e/o consenso del titolare degli stessi in conformità peraltro alle disposizioni normative di tempo in tempo vigenti.

La riservatezza è un bene che Web Consult S.r.l. tutela anche attraverso i propri collaboratori i quali sono tenuti a non utilizzare e/o divulgare a soggetti non autorizzati informazioni riservate per scopi non connessi con l'esercizio della propria attività. Per informazioni riservate si intendono, a titolo meramente esemplificativo, le informazioni tecniche relative a prodotti e procedure; le strategie aziendali, le relazioni finanziarie.

Il trattamento informatico delle informazioni è sottoposto ai controlli di sicurezza necessari a salvaguardare la società da indebite intrusioni od usi illeciti. La tutela della riservatezza delle informazioni richiede l'adozione di particolari norme comportamentali:

- non comunicare la propria password di accesso alla rete ed ai sistemi informatici di Web Consult S.r.l. e rispettare la normativa interna sulla sicurezza informatica;
- evitare le copie inutili di documenti riservati;
- evitare di mostrare i documenti riservati in locali ad accesso pubblico quali ascensori, sale d'attesa, ecc.;
- non abbandonare i documenti riservati sulle scrivanie o all'interno di sale riunioni o comunque laddove soggetti non autorizzati potrebbero prenderne visione;

- evitare discussioni che possano comportare la divulgazione di informazioni riservate in luoghi ad alta frequentazione quali ad esempio ascensori, ristoranti, mezzi di trasporto;
- accertarsi della tutela della riservatezza delle informazioni nei confronti di addetti professionali e di personale di supporto quale ad esempio addetti amministrativi, vettori e personale delle pulizie.

2.4. Sicurezza sul lavoro

Web Consult S.r.l. si impegna a tutelare la sicurezza e la salute nei luoghi di lavoro attuando quanto previsto dal D. Lgs. 81/08 e ritiene fondamentale, nell'espletamento della propria attività economica, il rispetto dei diritti dei lavoratori.

2.5. Tutela dell'ambiente

La tutela dell'ambiente e la salvaguardia delle risorse naturali sono importanti obiettivi aziendali: Web Consult S.r.l. si impegna affinché il comportamento di tutti i dipendenti, dei collaboratori e dei soggetti terzi con i quali la società intrattiene rapporti d'affari sono sia orientato al principio di rispetto e tutela dell'ambiente circostante.

2.6. Diffusione ed osservanza del Codice etico

La Società promuove la conoscenza e l'osservanza del Codice Etico, dei protocolli interni e dei loro aggiornamenti tra tutti gli amministratori, i dipendenti, i collaboratori a vario titolo, i consulenti, i clienti ed i fornitori, richiedendone il rispetto e prevedendo, in caso di inosservanza, adeguate sanzioni disciplinari o contrattuali. I soggetti sopra indicati sono pertanto tenuti a conoscere il contenuto del Codice Etico – chiedendo e ricevendo dalle funzioni aziendali preposte gli opportuni chiarimenti in merito alle interpretazioni del contenuto -, osservarli e contribuire alla loro attuazione, segnalando eventuali carenze e violazioni (o anche solo tentativi di violazione) di cui siano venuti a conoscenza. La Società inoltre promuove e incoraggia la collaborazione dei dipendenti nel far rispettare, conoscere ed attuare il Codice Etico e, nell'ambito delle rispettive competenze e funzioni, i protocolli interni.

2.7. Corporate Governance

La Società adotta un sistema di Corporate Governance conforme a quanto previsto dalla legge e dalle migliori prassi internazionali.

Tale sistema di governo societario è orientato alla massimizzazione del valore per gli azionisti, al controllo dei rischi d'impresa, alla trasparenza nei confronti del mercato. Eventuali modifiche della Corporate Governance che dovessero essere adottate a seguito dell'entrata in vigore della riforma societaria potranno comportare conseguenti modifiche del presente Codice Etico.

3. RISORSE UMANE E POLITICA DELL'OCCUPAZIONE

3.1. Le condizioni determinanti

Le risorse umane sono un elemento indispensabile per l'esistenza dell'Azienda. L'onestà, la lealtà, la capacità, la professionalità, la serietà, la preparazione tecnica e la dedizione del personale rientrano pertanto tra le condizioni determinanti per conseguire gli obiettivi della Società e rappresentano le caratteristiche richieste dall'Azienda ai propri amministratori, dipendenti e collaboratori a vario titolo.

3.2. Le politiche di selezione

Al fine di contribuire allo sviluppo degli obiettivi di impresa, ed assicurare che tali obiettivi siano da tutti perseguiti nel rispetto dei principi etici e dei valori cui la Società si ispira, la politica aziendale è volta a selezionare ciascun dipendente, consulente, collaboratore a vario titolo secondo i valori e le caratteristiche sopra enunciate. Nell'ambito della selezione – condotta nel rispetto delle pari opportunità e senza discriminazione alcuna sulla sfera privata e sulle opinioni dei candidati – la Società opera affinché le risorse acquisite corrispondano ai profili effettivamente necessari alle esigenze aziendali, evitando favoritismi e agevolazioni di ogni sorta.

3.3. Lo sviluppo delle professionalità

Nell'evoluzione del rapporto di lavoro la Società si impegna a creare e mantenere le condizioni necessarie affinché le capacità e le conoscenze di ciascuno possano ulteriormente ampliarsi nel rispetto di tali valori, seguendo una politica basata sul riconoscimento dei meriti e delle pari opportunità, e prevedendo specifici programmi volti all'aggiornamento professionale e dall'acquisizione di maggiori competenze. In ragione di ciò, al dipendente è richiesto di coltivare e sollecitare l'acquisizione di nuove competenze, capacità e conoscenze, mentre ai dirigenti ed ai responsabili di funzione è fatto obbligo di porre la massima attenzione nel valorizzare ed accrescere la professionalità dei propri collaboratori creando le condizioni per lo sviluppo delle loro capacità e la realizzazione delle loro potenzialità.

3.4. Risorse umane e Codice Etico

Attraverso proprie funzioni e risorse dedicate, la Società promuove e cura costantemente la conoscenza del Codice Etico, dei protocolli annessi e dei relativi aggiornamenti, nonché delle aree di attività delle diverse funzioni con attribuzioni di responsabilità, linee di dipendenza gerarchica, descrizione dei compiti e formazione del personale. L'informazione e la conoscenza del Codice Etico e dei relativi protocolli specifici avviene in primo luogo attraverso la distribuzione di apposita documentazione a tutti coloro che interagiscono con la Società. In secondo luogo la Società prevede per i propri dipendenti appositi programmi di formazione ed aggiornamento, curati dalle funzioni responsabili, sul Codice Etico e sui relativi protocolli. Il personale dell'Azienda potrà comunque, in qualsiasi momento, chiedere ai propri superiori consigli e chiarimenti sui contenuti del Codice Etico e dei protocolli e sulle mansioni ad essi attribuite. In occasione della costituzione di nuovi rapporti di lavoro, consulenza e/o collaborazione, la Società fornirà tempestivamente le informazioni necessarie ad una adeguata conoscenza del Codice Etico e dei protocolli, con particolare riferimento a quelli attinenti alle specifiche competenze.

3.5. Ambiente di lavoro e tutela della privacy

La Società si impegna a creare un ambiente di lavoro che garantisca, a tutti coloro che a qualunque titolo interagiscono con essa, condizioni rispettose della dignità personale e nel quale le caratteristiche dei singoli non possano dare luogo a discriminazioni o condizionamenti. Anche a questo proposito, nel rispetto della legislazione vigente, la Società si impegna alla tutela della privacy in merito alle informazioni attinenti la sfera privata e le opinioni di ciascuno dei propri dipendenti e, più in generale, di quanti interagiscono con l'Azienda. In particolare, il rispetto della dignità del lavoratore dovrà essere assicurato anche attraverso il rispetto della privacy nella corrispondenza e nelle relazioni interpersonali tra dipendenti, attraverso il divieto di interferenze in conferenze o dialoghi e attraverso il divieto di intromissioni o forme di controllo che possano ledere la personalità.

4. CONFLITTO DI INTERESSI

4.1. Interessi aziendali ed individuali

Tra la Società ed i propri dipendenti sussiste un rapporto di piena fiducia, nell'ambito del quale è dovere primario del dipendente utilizzare i beni dell'impresa e le proprie capacità lavorative esclusivamente per la realizzazione dell'interesse societario, in conformità ai principi fissati nel Codice Etico, che rappresentano i valori cui la Società si ispira. In tale prospettiva gli amministratori, i dipendenti ed i collaboratori a vario titolo della Società devono evitare ogni situazione ed astenersi da ogni attività che possa contrapporre un interesse personale a quelli della Azienda o che possa interferire ed intralciare la capacità di assumere, in modo imparziale ed obiettivo, decisioni nell'interesse dell'impresa. Il verificarsi di situazioni di conflitto di interessi, oltre ad essere in contrasto con le norme di legge e con i principi fissati nel Codice Etico, risulta pregiudizievole per l'immagine e l'integrità aziendale. Amministratori, dipendenti e collaboratori devono quindi escludere ogni possibilità di sovrapporre o comunque incrociare, strumentalizzando la propria posizione funzionale, le attività economiche rispondenti ad una logica di interesse personale e/o familiare e le mansioni che ricoprono all'interno della Società. In caso di violazione, la Società provvederà a porre in essere le misure idonee per far cessare la situazione.

4.2. Prevenzione dei conflitti di interesse

Al fine di evitare situazioni, anche potenziali, di conflitto di interesse, la Società al momento di assegnazione dell'incarico o di avvio del rapporto di lavoro richiede ai propri amministratori, dipendenti e collaboratori a vario titolo di sottoscrivere un'apposita dichiarazione che esclude la presenza di condizioni di conflitto di interesse tra singolo ed Azienda. Tale dichiarazione prevede inoltre che il soggetto si impegni ad informare tempestivamente la Società – nella figura del proprio superiore – nel caso in cui dovesse trovarsi in situazioni effettive o potenziali di conflitto di interessi.

5. PROCEDURE OPERATIVE E DATI CONTABILI

5.1. I protocolli specifici

Specifici protocolli, volti a prevenire eventi pregiudizievoli e conseguenti potenziali impatti negativi sulla situazione aziendale, sono ispirati dal codice di comportamento e sono predisposti- o opportunamente integrati e modificati – a seguito dell'analisi del contesto aziendale, volta ad evidenziare i rischi gravanti sull'Azienda ed il sistema di controllo esistente, nonché la sua effettiva adeguatezza. Protocolli specifici vanno adottati – da parte di tutti coloro che a qualunque titolo intervengono nel processo operativo - nei termini e nelle modalità appositamente previste e descritte dalle competenti funzioni della Società. La loro corretta attuazione garantisce la possibilità di identificare i soggetti aziendali responsabili del processo di decisione, autorizzazione e svolgimento delle operazioni: a tal fine – secondo il principio di controllo rappresentato dalla separazione dei compiti - è necessario che le singole operazioni siano svolte nelle varie fasi da soggetti diversi, le cui competenze sono chiaramente definite e conosciute all'interno dell'organizzazione, in modo da evitare che possano essere attribuiti poteri illimitati e/o eccessivi a singoli soggetti.

5.2. Osservanza delle procedure

Gli amministratori, con particolare riferimento agli amministratori esecutivi, i dipendenti e tutti coloro che intrattengono a qualsiasi titolo rapporti con la Società, ciascuno nell'ambito delle rispettive competenze e

funzioni, sono tenuti alla rigorosa osservanza delle procedure previste dai protocolli. In particolare le procedure aziendali devono regolamentare lo svolgimento di ogni operazione e transazione, di cui devono potersi rilevare (attraverso i seguenti elementi di controllo peraltro non esaustivi: quadrature, firme abbinate, documentazione contabile di supporto, approfondimenti su attività di agenti commerciali, consulenti, fornitori, etc), la legittimità, l'autorizzazione, la coerenza, la congruità, la corretta registrazione e verificabilità, anche sotto il profilo dell'utilizzo delle risorse finanziarie. Ogni operazione dovrà quindi essere supportata da adeguata, chiara e completa documentazione da conservare agli atti, in modo da consentire in ogni momento il controllo sulle motivazioni, le caratteristiche dell'operazione e la precisa individuazione di chi, nelle diverse fasi, l'ha autorizzata, effettuata, registrata e verificata. Il rispetto delle indicazioni previste dai protocolli specifici in merito al flusso procedurale da osservare sulla formazione, decisione e registrazione dei fenomeni aziendali e dei relativi effetti, consente tra l'altro di diffondere e stimolare a tutti i livelli aziendali la cultura del controllo, che contribuisce al miglioramento dell'efficienza gestionale e costituisce uno strumento di supporto all'azione manageriale. Eventuali inosservanze delle procedure previste dai protocolli e dal Codice Etico compromettono il rapporto fiduciario esistente tra la Società e coloro che, a qualsiasi titolo, interagiscono con essa.

5.3. Trasparenza contabile

Veridicità, accuratezza, completezza e chiarezza delle informazioni elementari rappresentano le condizioni necessarie che permettono un'attività di trasparente registrazione contabile e costituiscono un valore fondamentale per la Società, anche al fine di garantire a soci e terzi la possibilità di avere una immagine chiara della situazione economica, patrimoniale e finanziaria dell'impresa. Affinché tale valore possa essere rispettato è in primo luogo necessario che la documentazione dei fatti elementari, da riportare in contabilità a supporto della registrazione, sia completa, chiara, veritiera, accurata e valida, e venga mantenuta agli atti per ogni opportuna verifica. La connessa registrazione contabile deve riflettere in maniera completa, chiara, veritiera, accurata e valida ciò che è descritto nella documentazione di supporto. Nel caso di elementi economico-patrimoniali fondati su valutazioni, la connessa registrazione deve essere compiuta nel rispetto dei criteri di ragionevolezza e prudenza, illustrando con chiarezza nella relativa documentazione i criteri che hanno guidato la determinazione del valore del bene. Chiunque venga a conoscenza di possibili omissioni, falsificazioni, irregolarità nella tenuta della contabilità e della documentazione di base, o comunque di violazioni dei principi fissati dal Codice Etico e dai protocolli specifici è tenuto a riferirne tempestivamente al proprio superiore ovvero all'Organismo di Vigilanza. Le citate violazioni incrinano il rapporto di fiducia con la Società, assumono rilievo sotto il profilo disciplinare e saranno adeguatamente sanzionate.

6. TUTELA DEL PATRIMONIO SOCIALE

6.1. Custodia e gestione delle risorse

La Società si adopera affinché l'utilizzo delle risorse disponibili – effettuato in conformità alla normativa vigente ed ai contenuti dello statuto, ed in linea con i valori del Codice Etico – sia volto a garantire, accrescere e rafforzare il patrimonio aziendale, a tutela della società stessa, dei soci, dei creditori e del mercato.

I dipendenti ed i collaboratori esterni sono direttamente e personalmente responsabili della protezione e del legittimo utilizzo dei beni (fisici e immateriali) e delle risorse loro affidati per espletare le proprie funzioni.

Nessuno dei beni e delle risorse di proprietà dell'azienda deve essere utilizzato per finalità diverse da quelle indicate, né per finalità illegali.

Non è ammessa l'istituzione di fondi extra - contabili; ogni bene di proprietà dovrà venire registrato nelle scritture contabili, a meno che tale registrazione non sia esclusa dalla normativa vigente.

6.2. Operazioni illecite sulle azioni o sul capitale

A tutela dell'integrità del patrimonio sociale è in particolare fatto divieto, fuori dai casi in cui lo consenta espressamente la legge, di restituire in qualsiasi forma i conferimenti o liberare i soci dall'obbligo di eseguirli; di ripartire utili non effettivamente conseguiti o destinati per legge a riserva, ovvero riserve non distribuibili per legge; acquistare o sottoscrivere azioni o quote della società o di società controllanti; effettuare riduzioni del capitale sociale, fusioni o scissioni violando norme poste a tutela dei creditori; formare o aumentare fittiziamente il capitale sociale; soddisfare, in caso di liquidazione, le pretese dei soci in danno dei creditori sociali. Al fine di prevenire le fattispecie sopra richiamate la Società, nell'ambito dell'organizzazione aziendale, si adopera per la diffusione e la conoscenza delle norme di legge, del Codice Etico e dei protocolli annessi, prevedendo specifici programmi di informazione ed aggiornamento per gli amministratori ed i dipendenti sui reati in materia societaria.

7. RAPPORTI INTERGRUPPO

7.1. Autonomia e valori etici comuni

La Società opera in autonomia rispetto alle altre Società del Gruppo; ad esse richiede di operare nel rispetto dei valori espressi nel Codice Etico, in termini di collaborazione leale nel perseguimento degli obiettivi, nel rispetto della legge e delle normative vigenti. La Società evita di porre in essere comportamenti che, ancorché adottati nel proprio esclusivo interesse, risultino pregiudizievoli per l'integrità o l'immagine delle altre Società del Gruppo. Altresì la Società richiede che nessuna delle altre Società del Gruppo ponga in essere comportamenti o intraprenda decisioni che, pur determinando benefici a proprio favore, potrebbero risultare pregiudizievoli per l'integrità o l'immagine della Società.

7.2. Cooperazione e comunicazione intragruppo

Chi riveste cariche sociali od incarichi all'interno del Gruppo ha il dovere di partecipare assiduamente alle riunioni cui è invitato ad intervenire, di espletare gli incarichi a lui attribuiti con lealtà e correttezza, di favorire la comunicazione tra le aziende del Gruppo, di sollecitare ed utilizzare le sinergie intragruppo cooperando nell'interesse degli obiettivi comuni. La circolazione delle informazioni all'interno del Gruppo, in particolare ai fini della redazione del bilancio consolidato e di altre comunicazioni, deve avvenire conformemente ai principi di veridicità, lealtà, correttezza, completezza, chiarezza, trasparenza, prudenza, nel rispetto dell'autonomia di ciascuna società e degli specifici ambiti di attività.

8. ORGANISMO DI VIGILANZA

8.1. Attribuzioni e caratteristiche

Il compito di vigilare sul funzionamento e l'osservanza del Modello di organizzazione e gestione adottato dall'Azienda ai sensi del D.Lgs 231/01 e successive modificazioni è affidato all'Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e controllo, senza vincoli di subordinazione che ne possano in alcun modo limitare od impedire l'attività. L'Organismo di Vigilanza opera con imparzialità, autorità, continuità, professionalità, autonomia e a tal fine: è libero di accedere a tutte le fonti di informazione della Società; ha facoltà di prendere visione di documenti e consultare dati; suggerisce eventuali aggiornamenti del Codice Etico e dei protocolli interni, anche sulla base delle segnalazioni fornite dai dipendenti; può effettuare controlli, anche periodici, sul funzionamento e l'osservanza del Modello; è dotato di adeguata disponibilità

di risorse umane e materiali che gli consentono di operare in modo rapido ed efficiente. L'Organismo di Vigilanza opera inoltre con ampia discrezionalità e con il completo appoggio dei vertici della Società, con i quali collabora in assoluta indipendenza.

8.2. Segnalazioni all'Organismo di Vigilanza

Allo scopo di garantire l'effettività del Modello organizzativo attraverso specifici protocolli, la Società - nel rispetto della privacy e dei diritti individuali - predispone canali di informazione tramite i quali tutti coloro che vengano a conoscenza di eventuali comportamenti illeciti posti in essere all'interno dell'Azienda possano riferire, liberamente, direttamente ed in maniera riservata, all'Organismo di Vigilanza. A tale ente compete la verifica puntuale ed attenta delle notizie trasmesse, al fine di sottoporre la fattispecie in essere alla funzione aziendale competente per l'applicazione di eventuali sanzioni disciplinari o l'attivazione di meccanismi di risoluzione contrattuale.

9. RAPPORTI CON L'ESTERNO

9.1. RAPPORTI CON AUTORITA' ED ISTITUZIONI PUBBLICHE ED ALTRI SOGGETTI RAPPRESENTATIVI DI INTERESSI COLLETTIVI

9.1.1. Rapporti con Autorità e Pubbliche Amministrazioni

I rapporti attinenti all'attività della Società intrattenuti con pubblici ufficiali o con incaricati di pubblico servizio - che operino per conto della Pubblica Amministrazione, centrale e periferica, o di organi legislativi, delle istituzioni comunitarie, di organizzazioni pubbliche internazionali e di qualsiasi Stato estero - con la magistratura, con le autorità pubbliche di vigilanza e con altre autorità indipendenti, nonché con partners privati concessionari di un pubblico servizio, devono essere intrapresi e gestiti nell'assoluto e rigoroso rispetto delle leggi e delle normative vigenti, dei principi fissati nel Codice Etico e nei protocolli interni, in modo da non compromettere l'integrità e la reputazione di entrambe le parti. Attenzione e cura deve essere posta nei rapporti con i soggetti sopra indicati, in particolare nelle operazioni relative a: gare d'appalto, contratti, autorizzazioni, licenze, concessioni, richieste e/o gestione e utilizzazione di finanziamenti comunque denominati di provenienza pubblica (nazionale o comunitaria), gestione di commesse, rapporti con autorità di vigilanza o altre autorità indipendenti, enti previdenziali, enti addetti alla riscossione dei tributi, organi di procedure fallimentari, procedimenti civili, penali o amministrativi, ecc. Al fine di non compiere atti in contrasto con le norme di legge o comunque pregiudizievoli dell'immagine e dell'integrità dell'Azienda, le operazioni sopra richiamate e la correlata gestione delle risorse finanziarie devono, dalle funzioni aziendali specificamente autorizzate, essere intraprese nel dovuto rispetto delle leggi e dei principi del Codice Etico e nella completa osservanza dei protocolli interni.

9.1.2. Rapporti con organizzazioni politiche e sindacali

La Società non favorisce o discrimina direttamente o indirettamente alcuna organizzazione di carattere politico o sindacale. L'Azienda si astiene dal fornire qualsiasi contributo, diretto o indiretto, sotto qualsiasi forma, a partiti, movimenti, comitati ed organizzazioni politiche e sindacali, a loro rappresentanti e candidati, tranne quelli dovuti in base a specifiche disposizioni di legge.

9.1.3. Regali, benefici e promesse di favori

La Società vieta a tutti coloro che operano nel proprio interesse, in proprio nome o per proprio conto di accettare, offrire o promettere, anche indirettamente, denaro, doni, beni, servizi, prestazioni o favori non

dovuti (anche in termini di opportunità di impiego) in relazione a rapporti intrattenuti con pubblici ufficiali, incaricati di pubblico servizio o soggetti privati, per influenzarne le decisioni, in vista di trattamenti più favorevoli o prestazioni indebite o per qualsiasi altra finalità. Eventuali richieste o offerte di denaro o di favori di qualunque tipo (ivi compresi ad es. omaggi o regali di non modico valore) formulate indebitamente a coloro, o da coloro, che operano per conto della Società nel contesto di rapporti con la Pubblica Amministrazione (italiana o di paesi esteri) o con soggetti privati (italiani o esteri) devono essere portate immediatamente a conoscenza dell'Organismo di Vigilanza e della funzione aziendale competente per l'assunzione dei provvedimenti conseguenti.

9.2. RAPPORTI CON CLIENTI E FORNITORI

9.2.1. Condotta negli affari

Il rapporto corretto e trasparente con clienti e fornitori rappresenta aspetto rilevante del successo della Società. La selezione dei fornitori e gli acquisti di beni, merci e servizi devono avvenire secondo i principi del presente codice di comportamento e delle procedure interne, utilizzando la forma scritta e nel rispetto della struttura gerarchica del Gruppo. In ogni caso la selezione deve avvenire esclusivamente sulla base di parametri obiettivi quali la qualità, la convenienza, il prezzo, la capacità, l'efficienza. Nelle transazioni commerciali è richiesta ed imposta, anche in conformità a protocolli specifici, particolare attenzione al fine di evitare il pericolo di immissione tra il pubblico o ricezione di valori contraffatti o alterati.

Nello svolgimento della propria attività la Società intrattiene relazioni commerciali con clienti e fornitori solo in seguito ad un'approfondita verifica della loro onorabilità.

9.2.2. Regali, dazioni e benefici

Nei rapporti di affari con clienti e fornitori sono vietate dazioni, benefici (sia diretti che indiretti), omaggi, atti di cortesia e di ospitalità, salvo che siano di natura e valore tali da non compromettere l'immagine dell'Azienda e da non poter essere interpretati come finalizzati ad ottenere un trattamento di favore che non sia determinato dalle regole di mercato. In ogni caso, eventuali omaggi, atti di cortesia e di ospitalità devono essere comunicati e sottoposti alla decisione del superiore. Il dipendente che riceva, prometta od esegua doni o trattamenti di favore da clienti o fornitori che travalichino gli ordinari rapporti di cortesia, deve immediatamente avvertirne il superiore il quale ne darà immediata notizia agli specifici organi e/o alla competente funzione aziendale che, dopo le opportune verifiche, provvederanno, tramite le funzioni preposte a gestire la comunicazione verso l'esterno, ad informare l'autore del regalo, omaggio etc. sulla politica aziendale in materia.

10. INFORMATIVA SOCIETARIA

10.1. Disponibilità ed accesso alle informazioni

La Società, nei limiti stabiliti dalle normative vigenti fornisce con tempestività ed in modo completo le informazioni, i chiarimenti, i dati e la documentazione richiesti da soci, clienti, fornitori, autorità pubbliche di vigilanza, istituzioni, organi, enti ed altri stakeholders nello svolgimento delle rispettive funzioni. Ogni informazione societaria rilevante deve essere comunicata con assoluta tempestività sia agli Organi Societari deputati al controllo sulla gestione sociale, sia alle autorità di vigilanza. Una esaustiva e chiara comunicazione societaria costituisce garanzia, tra l'altro, della correttezza dei rapporti: con i soci, che devono poter agevolmente, in accordo con la normativa vigente, accedere ai dati informativi; con i terzi che vengono in contatto con l'Azienda, i quali devono poter avere una rappresentazione della situazione economica, finanziaria e patrimoniale dell'impresa; con le autorità di vigilanza, gli organi di revisione

contabile e di controllo interno che devono svolgere in modo efficace le attività di controllo, a tutela non solo dei soci, ma di tutto il mercato; con le altre società del Gruppo, anche ai fini della redazione del bilancio consolidato e di altre comunicazioni della Società.

10.2. Comunicazioni rilevanti e sollecitazione del mercato

Tramite le modalità e le funzioni designate nei protocolli interni la Società garantisce, a tutti coloro che sono legittimamente interessati alla conoscenza dei fatti aziendali ed alla prevista evoluzione della sua situazione economica, patrimoniale e finanziaria, l'accesso alle informazioni e la trasparenza delle scelte effettuate. Con riferimento agli azionisti la comunicazione di fenomeni o situazioni rilevanti dell'attività e della prevista evoluzione aziendale deve essere effettuata puntualmente. Particolare cura e correttezza è posta nella diffusione di comunicazioni rilevanti per la vita della Società che possano incidere in modo significativo sull'andamento del business o sulla credibilità e affidabilità della medesima presso società e/o banche. In proposito, protocolli specifici devono prevedere elementi di verifica e controllo, affinché le comunicazioni sociali previste per legge, le informazioni dirette ai soci o al pubblico sulla situazione aziendale e sulla attesa evoluzione economica, finanziaria e patrimoniale (sia della Società che del Gruppo), debbano sempre essere veritieri, privi di omissioni ed espongano fatti, ancorché oggetto di valutazioni, rispondenti al vero, in modo da non indurre in errore i destinatari delle informative.

11. RAPPORTI CON I MASS MEDIA E GESTIONE DELLE INFORMAZIONI

11.1. Modalità di condotta

I rapporti con la stampa, i mezzi di comunicazione ed informazione e, più in generale, gli interlocutori esterni, devono essere tenuti solo da soggetti espressamente a ciò delegati, in conformità alle procedure o regolamentazioni adottate dalla Società. Qualsiasi richiesta di notizie da parte della stampa o dei mezzi di comunicazione e informazione ricevuta dal personale della Società deve essere comunicata ai soggetti (funzioni aziendali) responsabili della comunicazione verso l'esterno, prima di assumere qualsivoglia impegno a rispondere alla richiesta. La comunicazione verso l'esterno deve seguire i principi guida della verità, correttezza, trasparenza, prudenza e deve essere volta a favorire la conoscenza delle politiche aziendali e dei programmi e progetti della Società. I rapporti con i mass media devono essere improntati al rispetto della legge, del Codice Etico, dei relativi protocolli e dei principi già delineati con riferimento ai rapporti con le istituzioni pubbliche e con l'obiettivo di tutelare l'immagine della Società.

11.2. Informazioni "price sensitive"

E' rigorosamente vietata ogni forma di investimento, diretto o per interposta persona, che trovi la sua fonte in notizie aziendali riservate. Particolare rilevanza ed attenzione deve essere, quindi, posta sulla comunicazione all'esterno di documenti, notizie ed informazioni inerenti a fatti che accadono nella sfera di attività diretta della Società, della Controllante e delle altre Società facenti parte del Gruppo Tecnocasa non di dominio pubblico ed idonee, se rese pubbliche, ad influenzare sensibilmente il prezzo degli strumenti finanziari e l'andamento del mercato azionario. La comunicazione di tali informazioni, dopo che gli amministratori od i responsabili all'uopo prepostine abbiano autorizzato la diffusione, avverrà sempre attraverso i canali ed i soggetti all'uopo preposti. In nessun caso, nella gestione delle informazioni, dovranno essere adottati comportamenti che possano favorire fenomeni di *insider trading* o di altra natura che abbiano quale conseguenza il depauperamento del patrimonio aziendale o siano volte ad arrecare indebiti vantaggi personali od a terzi.

12. VIOLAZIONI DEL CODICE ETICO – SISTEMA SANZIONATORIO

12.1. Segnalazioni delle violazioni

Con riferimento alla notizia di avvenuta, tentata o richiesta violazione delle norme contenute nel Codice Etico e nei protocolli annessi, sarà cura dell'Azienda garantire che nessuno, in ambito lavorativo, possa subire ritorsioni, illeciti condizionamenti, disagi e discriminazioni di qualunque tipo, per aver segnalato alle funzioni competenti la violazione dei contenuti del Codice Etico o delle procedure interne. Peraltro a seguito della segnalazione l'Azienda farà tempestivamente seguire opportune verifiche ed adeguate misure sanzionatorie.

12.2. Linee guida del sistema sanzionatorio

La violazione dei principi fissati nel Codice Etico e nelle procedure previste dai protocolli interni compromette il rapporto fiduciario tra la Società ed i propri amministratori, dipendenti, consulenti, collaboratori a vario titolo, clienti, fornitori. Tali violazioni saranno dunque perseguite dalla Società incisivamente, con tempestività ed immediatezza, attraverso provvedimenti disciplinari adeguati e proporzionati, indipendentemente dall'eventuale rilevanza penale di tali comportamenti e dall'instaurazione di un procedimento penale nei casi in cui costituiscano reato. Gli effetti delle violazioni del Codice Etico e dei protocolli interni devono essere pertanto tenuti in seria considerazione da tutti coloro che a qualsiasi titolo intrattengono rapporti con la Società: a tal fine l'Azienda provvede a diffondere il Codice Etico, i protocolli interni e ad informare sulle sanzioni previste in caso di violazione e sulle modalità e procedure di irrogazione. L'Azienda a tutela della propria immagine e a salvaguardia delle proprie risorse non intratterrà rapporti di alcun tipo con soggetti che non intendano operare nel rigoroso rispetto della normativa vigente, e/o che rifiutino di comportarsi secondo i valori ed i principi previsti dal Codice Etico ed attenersi alle procedure e regolamenti previsti dai protocolli annessi.

12.3. Misure nei confronti dei lavoratori subordinati cui si applicano i contratti collettivi (C.C.N.L.) per il settore

Ai lavoratori subordinati si applicano le sanzioni disciplinari previste dal C.C.N.L., nel rispetto delle procedure previste dall'art. 7 dello Statuto dei Lavoratori.

In applicazione dei principi generali sopra indicati, la violazione delle norme del Codice può comportare l'applicazione delle sanzioni del RIMPROVERO SCRITTO, della Multa, della SOSPENSIONE o del LICENZIAMENTO per giustificato motivo o per giusta causa.

La contestazione delle infrazioni è effettuata dall'organo amministrativo; i procedimenti disciplinari e l'irrogazione delle sanzioni rientrano, nei limiti della competenza, nelle attribuzioni dei soggetti ai quali vengono dalla Direzione aziendale conferiti i relativi poteri.

12.4. Misure nei confronti dell'Organo Amministrativo ed Alta Direzione

In caso di grave violazione delle norme del Codice da parte delle funzioni apicali è prevista una formale informativa da parte dell'ODV all'Organo Amministrativo per l'opportuna valutazione.

12.5. Misure nei confronti di consulenti e fornitori

La violazione delle norme del Codice da parte di Consulenti o di Fornitori comporterà, per le funzioni aziendali che con gli stessi intrattengono rapporti, l'obbligo di azionare tutti gli strumenti contrattuali e di legge a disposizione per la tutela dei diritti dell'azienda, ivi compresi, ove del caso, la risoluzione del contratto ed il risarcimento dei danni.

STRUTTURA ORGANIZZATIVA DI
TECNOLOGICA S.r.l. (già Web Consult S.r.l.)

CONSIGLIO DI AMMINISTRAZIONE

PASQUALI Anna	Presidente
DE PALMA Dario	Consigliere Delegato
PEREZ LUNA Miguel Angel	Consigliere

ORGANISMO DI VIGILANZA

PICCIOLO Gaetano	Esperto legale in materia
-------------------------	----------------------------------