

# **DIGITAL SOLUTIONS**

**Modello di organizzazione, gestione e controllo  
ai sensi del Decreto Legislativo 231/2001**

**PARTE SPECIALE**

# DIGITAL SOLUTIONS

PARTE SPECIALE A.....	3
A.1. Funzione della Parte Speciale A.....	4
A.2. Fattispecie di Reato rilevanti.....	4
A.3. Criteri per la definizione di Pubblica Amministrazione e di soggetti incaricati di pubblico servizio.....	8
A.4. Aree a Rischio ed Attività Sensibili.....	12
A.5. Regole Generali.....	12
A.6. Principi generali di comportamento.....	14
A.7. Principi specifici di comportamento.....	15
PARTE SPECIALE B.....	21
B.1. Funzione della Parte Speciale B.....	22
B.2. Fattispecie di Reato rilevanti.....	22
B.3. Aree a Rischio ed Attività Sensibili.....	25
B.4. Principi generali di comportamento.....	26
B.5. Principi specifici di comportamento.....	27
PARTE SPECIALE C.....	31
C.1. Funzione della Parte Speciale C.....	32
C.2.1. Fattispecie di “ <i>corruzione tra privati</i> ” e “ <i>istigazione alla corruzione tra privati</i> ”.....	32
C.3. Aree di Rischio e Attività Sensibili.....	33
C.4. Regole e principi generali di comportamento.....	36
C.5. Principi specifici di comportamento.....	37
PARTE SPECIALE D.....	40
D.1. Funzione della Parte Speciale D.....	41
D.2. Le fattispecie di Reato.....	41
D.3. Aree di Rischio ed Attività Sensibili.....	47
D.4. Principi generali di comportamento.....	48
D.5. Principi specifici di comportamento.....	49
PARTE SPECIALE E.....	52
E.1 Funzione della Parte Speciale E.....	53
E.2 Fattispecie di Reato rilevanti.....	53
E.3 Aree di rischio ed Attività Sensibili.....	55
E.4 Principi generali di comportamento.....	55
E.5 Principi Specifici di comportamento.....	55
PARTE SPECIALE F.....	57
F.1. Funzione della Parte Speciale F.....	60
F.2. Fattispecie di Reato rilevanti.....	60
F.3. Aree di Rischio ed Attività Sensibili.....	61
F.4. Il sistema di prevenzione in generale.....	62
F.5. Presidi in tema di sicurezza e selezione ed assunzione del personale.....	73
PARTE SPECIALE G.....	75
G.1 Funzione della Parte Speciale G.....	76
G.2 Fattispecie di reato rilevanti.....	76
G.2.1 Delitti Tributari.....	76
G.3 Aree di Rischio ed Attività Sensibili.....	77
G.4 Principi generali di comportamento.....	78
G.5 Principi specifici di comportamento.....	78

**PARTE SPECIALE A**

**REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA  
AMMINISTRAZIONE**

**E**

**REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI  
O A RENDERE DICHIARAZIONI MENDACI  
ALL'AUTORITA' GIUDIZIARIA**

**Articoli 24, 25 e 25-*decies* del Decreto Legislativo 231/2001**

## DIGITAL SOLUTIONS

### A.1. Funzione della Parte Speciale A.

La presente Parte Speciale si riferisce ai comportamenti posti in essere dai Dipendenti, dai componenti degli Organi Sociali, da Consulenti, *Partner* e Terzi come già definiti nella Parte Generale.

L'obiettivo è che tutti i Destinatari come sopra individuati adottino regole di condotta conformi a quanto prescritto, al fine di prevenire il verificarsi dei Reati di cui agli articoli 24, 25 e 25-*decies* del Decreto.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- a) indicare le procedure che i Destinatari sono chiamati ad osservare al fine di applicare correttamente le prescrizioni del Modello;
- b) fornire all'*Executive Committee*, ai responsabili delle funzioni interne quali gli Organi Sociali o soggetti che cooperano con tali funzioni, nonché all'OdV, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

### A.2. Fattispecie di Reato rilevanti.

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la Pubblica Amministrazione, nonché al reato di induzione del soggetto chiamato dall'autorità giudiziaria a non rendere dichiarazioni o a rendere dichiarazioni mendaci utilizzabili nel procedimento in forza di un comportamento minaccioso o di un accordo.

Si descrivono qui di seguito le singole fattispecie contemplate negli articoli 24, 25 e 25-*decies* del Decreto Legislativo 231/2001, cui seguono casi di esempio di condotte criminose rilevanti.

Con il Decreto Legislativo n. 75 del 14 luglio 2020, recependo la Direttiva UE 2017/1371 (c.d. PIF) sono state introdotte nell'ordinamento norme per la "*lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale*". Tra le novità introdotte, si segnala la modifica del Decreto 231/2001 con l'aggiunta di nuovi reati presupposto. Per quel che attiene la presente sezione A della parte speciale, si è ritenuto fosse fattispecie rilevante tra i nuovi reati introdotti la sola frode nelle pubbliche forniture ex art. 356 c.p., omettendo le ulteriori fattispecie.

#### A.2.1. Reati contro la Pubblica Amministrazione.

##### **Malversazione a danno dello Stato (articolo 316-*bis* del Codice Penale).**

Il reato si configura nel caso in cui, dopo avere legittimamente ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta; nessun rilievo assume il fatto che l'attività programmata si sia comunque svolta).

##### **Indebita percezione di erogazioni in danno dello Stato (articolo 316-*ter* del Codice Penale).**

Il reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o 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.

## DIGITAL SOLUTIONS

In questo caso, contrariamente al reato di cui all'articolo 316-*bis* del Codice Penale, a nulla rileva l'uso che venga successivamente fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Questa ipotesi di reato è residuale rispetto alla più grave fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa aggravata per il percepimento di erogazioni pubbliche e dunque non si concretizzi in "artifici" o raggiri" ma in una mera condotta omissiva o semplice mendacio.

### **Frode nelle pubbliche forniture (Articolo 356 Codice Penale)**

Il reato si configura nel caso in cui, nell'esecuzione di un contratto di fornitura conclusa con lo Stato o altro ente pubblico o dell'Unione Europea o esercente servizi di pubblica necessità o nell'adempimento di altri obblighi contrattuali venga commessa frode. Detto reato può comportare la responsabilità dell'ente ai sensi del Decreto

### **Concussione (articolo 317 del Codice Penale).**

Il reato si configura nel caso in cui un pubblico ufficiale, abusando della propria posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli.

Questo reato è suscettibile di un'applicazione meramente residuale rispetto ad altre fattispecie considerate dal Decreto; in particolare, tale forma di reato potrebbe ravvisarsi nell'ipotesi in cui un Dipendente od un agente della società, concorra nel reato commesso dal pubblico ufficiale, il quale, approfittando di tale sua qualità, richieda a terzi prestazioni non dovute (sempre che tale comportamento sia posto in essere nell'interesse, anche non esclusivo, della società).

### **Corruzione per l'esercizio della funzione (articolo 318 del Codice Penale).**

Il reato si configura nel caso in cui un pubblico ufficiale per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

### **Corruzione per un atto contrario ai doveri d'ufficio (articoli 319, 319-bis e 321 del Codice Penale).**

Il reato si configura nel caso in cui un pubblico ufficiale per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve per sé o per un terzo, in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa.

### **Corruzione in atti giudiziari (articolo 319-ter e 321 del Codice Penale).**

Il reato si potrebbe configurare nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere o altro funzionario). Il reato in parola è punito più gravemente della corruzione semplice.

### **Induzione indebita a dare o promettere utilità (articolo 319-quater del Codice Penale).**

La norma punisce il pubblico ufficiale o l'incaricato di pubblico servizio che abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità, salvo che il fatto costituisca più grave reato.

### **Corruzione di persona incaricata di pubblico servizio (articolo 320 del Codice Penale).**

Le disposizioni degli articoli 318 e 319 del Codice Penale si applicano anche all'incaricato di un pubblico servizio.

### **Istigazione alla corruzione (articolo 322 del Codice Penale).**

Vi incorre chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri qualora l'offerta o la promessa non sia accettata.

Vi incorre chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, se l'offerta o la promessa è fatta per indurre ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, qualora l'offerta o la promessa non sia accettata.

### **Truffa a danno dello Stato o di altro Ente Pubblico o delle Comunità Europee (articolo 640, comma 2, n. 1 del Codice Penale).**

Il reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea).

Il reato può realizzarsi, ad esempio, nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (per esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

### **Truffa aggravata per il conseguimento di erogazioni pubbliche (articolo 640-bis del Codice Penale).**

Il reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.

Questa 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 (articolo 640-ter del Codice Penale).**

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

### **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (articolo 322-bis del Codice Penale).**

Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

- i) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- ii) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- iii) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- iv) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

## DIGITAL SOLUTIONS

- v) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

Le disposizioni degli articoli 319-*quater*, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

- i) alle persone indicate nel primo comma del presente articolo;
- ii) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

### A.2.2. Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

#### **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (articolo 377-bis del Codice Penale).**

Il reato si configura allorché taluno, con violenza, minaccia, con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci alla persona chiamata a rendere, davanti alla autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale, quando questa ha facoltà di non rispondere<sup>1</sup>, salvo che il fatto costituisca più grave reato.

### A.3. Criteri per la definizione di Pubblica Amministrazione e di soggetti incaricati di pubblico servizio.

Il presente capitolo ha come obiettivo quello di indicare quali siano i criteri generali che i Destinatari devono rispettare nonché quello di specificare che l'ente è responsabile solo qualora i reati vengano commessi nel suo interesse o suo vantaggio da soggetti previsti all'articolo 5, comma 1, lettera a) e b), Decreto Legislativo 231/2001, ovvero: *“a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione, il controllo dello stesso; oppure b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a<sup>2</sup>)”*.

#### A.3.1. Enti della Pubblica Amministrazione.

Agli effetti della legge penale, viene comunemente considerato come *“Ente della Pubblica Amministrazione qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi. Sebbene non esista nel codice penale una definizione di Pubblica Amministrazione, in base a quanto stabilito nella Relazione Ministeriale al codice stesso ed in relazione ai reati in esso previsti, sono ritenuti appartenere alla pubblica amministrazione quegli enti che svolgano “tutte le attività dello Stato e degli altri enti pubblici”*.

<sup>1</sup> Si tratta di soggetti che rivestono la qualifica di indagato (o imputato), dei loro prossimi congiunti a cui la legge conferisce la facoltà di non rispondere, ai sensi dell'articolo 199 del Codice di Procedura Penale e dei soggetti che assumono la veste di indagato (o imputato) di reato connesso o collegato, sempre che gli stessi non abbiano già assunto l'ufficio di testimone.

<sup>2</sup> La società non risponde se le persone indicate nel comma primo hanno agito nell'interesse esclusivo proprio o di terzi.



## DIGITAL SOLUTIONS

Nel tentativo di formulare una preliminare classificazione di soggetti giuridici appartenenti a tale categoria è possibile richiamare, da ultimo, l'articolo 1, comma secondo del Decreto Legislativo 30 marzo 2001, n. 165 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

A titolo esemplificativo, si possono indicare quali soggetti della Pubblica Amministrazione, i seguenti enti o categorie di enti:

- i) istituti e scuole di ogni ordine e grado e le istituzioni educative;
- ii) enti ed amministrazioni dello Stato ad ordinamento autonomo, quali:
  - organi istituzionali (Camera e Senato) e poteri dello Stato (Magistratura ordinaria e amministrativa), organi della Pubblica Amministrazione (Ministeri) ed enti amministrativi (Agenzia delle Entrate);
  - Regioni Province e Comuni;
  - società a partecipazione pubblica, statale (es. ENI, ENEL) o locale (società regionali o municipalizzate);
  - Autorità di Vigilanza (quali ad esempio Banca d'Italia, Consob, AGCM);
  - Camera di Commercio, Industria, Artigianato e Agricoltura e loro associazioni;
  - tutti gli enti pubblici non economici nazionali, regionali, e locali (quali, ad esempio INPS, CNR, INAIL, ISTAT, ENASARCO);
  - ASL;
  - Enti e Monopoli di Stato;
  - soggetti di diritto privato che esercitano un pubblico servizio (ad esempio, Cassa Depositi e Prestiti, Ferrovie dello Stato, Enel, Accredia);
  - fondazioni di previdenze ed assistenza.

Quindi, si noti come anche i soggetti di diritto privato concessionari di pubblici servizi e le società partecipate a maggioranza da un ente pubblico sono considerate, dalla più recente giurisprudenza, alla stessa stregua di enti pubblici.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose ex Decreto Legislativo 231/2001.

In particolare le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio"<sup>3</sup>.

---

<sup>3</sup> Rileva comunque precisare che la qualifica di Pubblico Ufficiale o di Incaricato di Pubblico Servizio del soggetto passivo non è sempre indispensabile ai fini della configurazione dei reati in esame; si pensi a tal proposito al reato di truffa aggravata per il conseguimento di erogazioni pubbliche ex articolo 640-bis Codice Penale in cui soggetti passivi sono lo Stato, altri enti pubblici o Comunità Europee.

### A.3.1.1 Pubblici Ufficiali.

Ai sensi dell'articolo 357, primo comma del Codice Penale, è considerato pubblico ufficiale *“agli effetti della legge penale”* colui il quale esercita *“una pubblica funzione legislativa, giudiziaria o amministrativa”* precisando che *“è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autorizzativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”*.

Il secondo comma si preoccupa poi di definire la nozione di “pubblica funzione amministrativa”. Non si è compiuta invece un’analoga attività definitoria per precisare la nozione di “funzione legislativa” e “funzione giudiziaria” in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.

Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale *“è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”*.

Tale ultima definizione normativa individua, innanzitutto, la delimitazione “esterna” della funzione amministrativa. Tale delimitazione è attuata mediante il ricorso a un criterio formale che fa riferimento alla natura della disciplina, per cui è definita pubblica la funzione amministrativa disciplinata da “norme di diritto pubblico”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Inoltre, il secondo comma dell'articolo 357 del Codice Penale traduce in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di “pubblica funzione” da quella di “servizio pubblico”. Vengono quindi pacificamente definite come “funzioni pubbliche” quelle attività amministrative che rispettivamente ed alternativamente costituiscono esercizio di: (a) poteri deliberativi; (b) poteri autoritativi; (c) poteri certificativi.

Alla luce dei principi sopra enunciati, si può affermare che la categoria di soggetti più problematica è certamente quella che ricopre una “pubblica funzione amministrativa”.

Per fornire un contributo pratico alla risoluzione di eventuali “casi dubbi”, può essere utile ricordare che assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico amministrativo dello Stato o di enti territoriali, ma anche – sempre riferendoci ad un’attività di altro ente pubblico retta da norme pubblicistiche – tutti coloro che, in base allo statuto nonché alle deleghe che esso consenta, ne formino legittimamente la volontà e/o la portino all'esterno in forza di un potere di rappresentanza (e.g. i componenti di un consiglio di amministrazione di un ospedale: Cass. Pen., Sez. VI, 15 dicembre 1997, n. 11462).

Sembra esatto infine affermare, in tale contesto, che non assumono la qualifica in esame altri soggetti che svolgono solo mansioni preparatorie alla formazione della volontà dell'ente (e così, i segretari amministrativi, i geometri, i ragionieri e gli ingegneri, tranne che, in specifici casi e per singole incombenze, non “formino” o manifestino la volontà della Pubblica Amministrazione).

#### **Reati che possono essere commessi solo da o verso pubblici ufficiali:**

Articolo 317	del Codice Penale	Concussione
Articolo 318	del Codice Penale	Corruzione per un atto d'ufficio
Articolo 319	del Codice Penale	Corruzione per un atto contrario ai doveri d'ufficio

Articolo 319-ter del Codice Penale Corruzione in atti giudiziari

Articolo 322 del Codice Penale Istigazione alla corruzione

### A.3.1.2. Incaricati di un pubblico servizio.

La definizione della categoria di “soggetti incaricati di un pubblico servizio” si rinviene all’articolo 358 del Codice Penale il quale recita che “*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*”.

Il legislatore puntualizza la nozione di “pubblico servizio” attraverso due ordini di criteri, uno positivo ed uno negativo. Il “*servizio*”, affinché possa definirsi pubblico, deve essere disciplinato – del pari alla “*pubblica funzione*” – da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione. Esempi di incaricati di pubblico servizio sono: i dipendenti delle autorità di vigilanza che non concorrono a formare la volontà dell’autorità e che non hanno poteri autoritativi, i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, etc..

Il legislatore ha, inoltre, precisato che non può mai costituire “servizio pubblico” lo svolgimento di “*semplici mansioni di ordine*” né la “*prestazione di opera meramente materiale*”. Con riferimento alle attività che vengono svolte da soggetti privati in base ad un rapporto concessorio con un soggetto pubblico, si ritiene che ai fini della definizione come pubblico servizio dell’intera attività svolta nell’ambito di tale rapporto concessorio non è sufficiente l’esistenza di un atto autoritativo di investitura soggettiva del pubblico servizio, ma è necessario accertare se le singole attività che vengono in questione siano a loro volta soggette a una disciplina di tipo pubblicistico.

La giurisprudenza ha individuato la categoria degli incaricati di un pubblico servizio, ponendo l’accento sul carattere della strumentalità ed accessorietà delle attività rispetto a quella pubblica in senso stretto.

Essa ha quindi indicato una serie di “*indici rivelatori*” del carattere pubblicistico dell’ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

- i) la sottoposizione ad un’attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;
- ii) la presenza di una convenzione e/o concessione con la Pubblica Amministrazione;
- iii) l’apporto finanziario da parte dello Stato;
- iv) l’immanenza dell’interesse pubblico in seno all’attività economica.

Sulla base di quanto sopra riportato, l’elemento discriminante per indicare se un soggetto rivesta o meno la qualifica di “incaricato di un pubblico servizio” è rappresentato, non dalla natura giuridica assunta o detenuta dall’ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

In tal senso da ultimo si è espresso anche il Consiglio di Stato con Sentenza n. 1094, depositata in Cancelleria il 13 marzo 2008 (ribadendo, in tale sede, che lo svolgimento dell’attività sociale, esercitata in regime di concessione amministrativa da una società per azioni di diritto privato – nel

## DIGITAL SOLUTIONS

caso di specie, la costruzione e la gestione delle autostrade – con finalità oggettivamente pubbliche ha natura di attività amministrativa e non di attività di diritto privato).

### **Reati che possono essere ascritti agli incaricati di pubblico servizio:**

Articolo 317	del Codice Penale	Concussione
Articolo 318	del Codice Penale	Corruzione per un atto d'ufficio
Articolo 319	del Codice Penale	Corruzione per un atto contrario ai doveri d'ufficio
Articolo 319-ter	del Codice Penale	Corruzione in atti giudiziari
Articolo 322	del Codice Penale	Istigazione alla corruzione

### **A.4. Aree a Rischio ed Attività Sensibili.**

Le Aree a Rischio ed Attività Sensibili che la Società ha individuato al proprio interno, con riferimento ai Reati già esposti nella presente Parte Speciale sono le seguenti:

- *Rapporti con la P.A. e soggetti incaricati di un pubblico servizio per l'adempimento degli obblighi di legge (i.e. rapporti con l'Agenzia delle Entrate per adempimenti fiscali e contributivi);*
- *Gestione delle attività di sviluppo mediante gare pubbliche, solicited bid o trattative private;*
- *Gestione della selezione, assunzioni del personale e del sistema premiante;*
- *Gestione del contenzioso e dei rapporti con l'Autorità giudiziaria e ispezioni;*
- *Gestione degli acquisti e delle consulenze.*

I Destinatari sono tenuti ad adeguare il proprio comportamento a quanto esposto nel Codice Etico e nel presente Modello.

### **A.5. Regole Generali.**

#### **A.5.1. Il sistema in linea generale.**

Tutte le Attività Sensibili indicate nelle Aree a Rischio devono essere svolte in conformità delle leggi vigenti, al Codice Etico, ai valori e ai principi comportamentali della Società e alle regole contenute nel presente Modello.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, etc.) improntati a principi generali di:

- i) conoscibilità all'interno della Società;
- ii) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;

## DIGITAL SOLUTIONS

iii) chiara descrizione dei flussi informativi all'interno della Società.

Le procedure interne sono caratterizzate dai seguenti elementi:

- i) massima separatezza possibile, compatibilmente con le risorse disponibili, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e lo conclude, e il soggetto che lo controlla;
- ii) traccia scritta di ciascun passaggio rilevante del processo;
- iii) adeguato livello di formalizzazione;
- iv) i sistemi premianti dei soggetti dotati di poteri di spesa o facoltà decisionali a rilevanza esterna, quando esistenti, siano basati su *target di performance* sostanzialmente raggiungibili.

### A.5.2. Il sistema di deleghe e procure.

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di “sicurezza” ai fini della prevenzione dei reati cd. presupposto (rintracciabilità ed evidenziabilità delle Attività Sensibili svolte all'interno delle Aree a Rischio) e, nel contempo, consentire comunque la gestione efficiente della struttura operativa.

Si intende per “*delega*” l'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per “*procura*” il negozio giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

Ai titolari di una funzione, che necessitano per lo svolgimento dei loro incarichi di poteri di rappresentanza, viene conferita una “procura generale funzionale” di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la “delega”.

I requisiti essenziali del sistema di deleghe, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

- i) tutti coloro (compresi anche i Dipendenti o gli Organi Sociali) che intrattengono per conto della Società rapporti con la P.A. devono essere dotati di delega formale in tal senso;
- ii) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- iii) ciascuna delega deve definire in modo specifico ed inequivoco:
  - i poteri del delegato;
  - il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;
  - i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi imprenditoriali della Società;
- iv) il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di un'efficace prevenzione dei Reati, sono i seguenti:

## DIGITAL SOLUTIONS

- i) le procure generali funzionali sono conferite esclusivamente a soggetti dotati di delega interna;
- ii) le procure generali descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione organizzativa che fissi: l'estensione di poteri di rappresentanza ed i limiti di spesa numerici; ovvero i limiti assuntivi per categorie di rischio, richiamando comunque il rispetto dei vincoli posti dai processi di approvazione del *budget* e degli eventuali *extra budget*, dai processi di determinazione dei poteri assuntivi, dai processi di monitoraggio delle Aree a Rischio da parte di funzioni diverse;
- iii) la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;
- iv) le procure speciali devono dettagliatamente stabilire l'ambito di operatività e i poteri del procuratore;
- v) una procedura *ad hoc* deve disciplinare modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le procure devono essere attribuite, modificate e revocate (assunzione o estensione di nuove responsabilità e poteri, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, revoca, etc.).

L'OdV verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni all'ente con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

### A.6. Principi generali di comportamento.

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari ovvero che si applicano ai Dipendenti ed agli Organi Sociali – in via diretta – sia ai Consulenti, ai *Partner* ed ai Terzi in forza di apposite clausole contrattuali.

In generale, è fatto divieto di porre in essere comportamenti o concorrere o dare causa alla realizzazione di condotte tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate di cui agli articoli 24 e 25 e 25-*decies* del Decreto Legislativo 231/2001; sono altresì proibite le violazioni ai principi ed alle procedure previste nella presente Parte Speciale e nel Codice Etico.

Nell'ambito dei suddetti comportamenti è fatto divieto (coerentemente a quanto previsto anche nel Codice Etico) in particolare di:

- i) effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
- ii) offrire doni o gratuite prestazioni al di fuori di quanto previsto dalle prassi in vigore nella Società (vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia ovvero di un valore superiore ad Euro 150,00 (centocinquanta/00) o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività imprenditoriale). In particolare, ai rappresentanti della P.A. e/o autorità pubbliche o a loro familiari non deve essere offerta, né direttamente né indirettamente, alcuna forma di regalo, doni o gratuite prestazioni che possano apparire, comunque, connessi con il rapporto di affari

con la Società o miranti ad influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società.

Anche in quei Paesi in cui offrire regali o doni costituisce una prassi diffusa in segno di cortesia, tali regali devono essere di natura appropriata e non contrastare con le disposizioni di legge; non devono comunque essere interpretati come richiesta di favori in contropartita. In caso di dubbio il destinatario deve darne tempestiva informazione alla funzione competente, la quale sottoporrà la segnalazione al Consiglio di Amministrazione ovvero all'Amministratore Delegato. In tali casi si deve prontamente informare l'OdV anche mediante un'elencazione dettagliata dei regali offerti;

- iii) accordare vantaggi di qualsiasi natura in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le stesse conseguenze previste al precedente punto ii);
- iv) eseguire prestazioni e riconoscere compensi in favore dei Consulenti, dei *Partner* e dei Terzi che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi.

### A.7. Principi specifici di comportamento.

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente Capitolo, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole già contenute nella Parte Generale del Modello.

Le regole qui di seguito descritte devono essere rispettate sia nell'esplicazione dell'attività della Società in territorio italiano, sia eventualmente all'estero.

- ***Gestione dei rapporti con la P.A. e soggetti incaricati di un pubblico servizio per l'adempimento dell'obbligo di legge***

La gestione dei rapporti con la P.A. nell'ambito delle operazioni ordinarie ovvero negli adempimenti amministrativi può presentare taluni fattori di rischio facilmente mitigabili attraverso sia:

- i) la dotazione di procedure formalizzate che specifichino le modalità in cui ci si debba confrontare ed interagire con la P.A. (in questo caso trattasi di Enti quali Agenzia delle Entrate, INPS, INAIL, ASL, Camera di Commercio nonché enti comunali, etc.);
- ii) l'individuazione e incarico formale dei soggetti delegati ad interfacciarsi con la P.A. in nome e per conto della Società.

Tale rischio si realizza nell'ipotesi in cui un soggetto sottoposto o apicale di Digital Solutions offrisse o promettesse denaro o altra utilità ad un pubblico ufficiale, ad un incaricato di pubblico servizio o a soggetti da questi indicati, per compiere, ritardare od omettere un atto del proprio ufficio oppure qualora un soggetto sottoposto o apicale di Digital Solutions inducesse in errore un pubblico ufficiale mediante artifici o raggiri (quali, ad esempio, la falsificazione o l'alterazione dei documenti predisposti per la P.A.) al fine di ottenere un ingiusto profitto con danno della P.A..

- ***Gestione delle attività di sviluppo mediante gare pubbliche, solicited bid o trattative private.***

La gestione delle attività di sviluppo mediante gare d'appalto (pubbliche o private), *solicited bid* o trattative private, la gestione delle operazioni di implementazione dei progetti, nonché la gestione degli adempimenti amministrativi e delle relative attività ispettive potrebbero presentare profili di rischio in relazione alla commissione dei reati contro la Pubblica Amministrazione.



## DIGITAL SOLUTIONS

Tale rischio si realizza nell'ipotesi in cui un soggetto sottoposto o apicale di Digital Solutions offrisse o promettesse denaro o altra utilità ad un pubblico ufficiale, ad un incaricato di pubblico servizio o a soggetti da questi indicati, per compiere, ritardare od omettere un atto del proprio ufficio oppure qualora un soggetto sottoposto o apicale di Digital Solutions inducesse in errore un pubblico ufficiale mediante artifici o raggiri (quali, ad esempio, la falsificazione o l'alterazione dei documenti predisposti per la P.A.) al fine di ottenere un ingiusto profitto con danno della P.A..

Ai Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione dei rapporti con la Pubblica Amministrazione, con le *Authorities*, è fatto obbligo:

- i) di assicurare che i suddetti rapporti avvengano nell'assoluto rispetto di:
  - leggi;
  - normative vigenti;
  - il Modello;
  - il Codice Etico;
  - principi di lealtà, correttezza e chiarezza;
- ii) di garantire che l'*iter* decisionale, per la realizzazione di nuove iniziative, sia adeguatamente approvato da parte dei comitati della Società, nonché dall'Amministratore Delegato ovvero dal Consiglio di Amministrazione;
- iii) di ottenere tutte le autorizzazioni necessarie alla realizzazione dei progetti;
- iv) di garantire che sia verificata la conformità dei progetti ai requisiti normativi prima della messa in funzione;
- v) di assicurare che la documentazione sia predisposta dalle persone competenti in materia e preventivamente identificate;
- vi) di assicurare che i rapporti con funzionari della Pubblica Amministrazione o di amministrazioni private siano gestiti esclusivamente dai soggetti muniti di idonei poteri;
- vii) nel caso in cui la documentazione da inviare alla P.A. sia prodotta – in tutto o in parte – con il supporto di soggetti terzi (ad esempio: consulenti tecnici, etc.), di garantire che la selezione degli stessi avvenga sempre nel rispetto di quanto disciplinato nella sezione "*Gestione acquisti di beni o servizi (incluse le consulenze)*" della presente Parte Speciale;
- viii) di assicurare la tracciabilità dei rapporti intrattenuti con le P.A.;
- ix) di comunicare, senza ritardo, al proprio responsabile gerarchico o al *management* della Società e contestualmente all'Organismo di Vigilanza, eventuali comportamenti posti in essere da quanti operano con la controparte pubblica o privata, rivolti ad ottenere favori, elargizioni illecite di danaro od altre utilità, anche nei confronti dei terzi, nonché qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A.;
- x) di sottoporre ai soggetti muniti di idonei poteri, in base al sistema di procure e deleghe in essere, la documentazione da trasmettere alle P.A. al fine di verificarne validità, completezza e veridicità.



Nell'ambito dei citati comportamenti è fatto divieto di:

- i) intrattenere rapporti con funzionari della Pubblica Amministrazione o pubblici ufficiali senza la presenza di almeno un'altra persona, ove possibile, e senza garantire la tracciabilità, come sopra specificato;
  - ii) effettuare promesse o indebite elargizioni di denaro o altra utilità (a titolo esemplificativo: assunzioni, conferimenti di incarichi di natura professionale, commerciale o tecnica) a pubblici funzionari, incaricati di pubblico servizio, soggetti privati o persone a questi ultimi vicini;
  - iii) cedere a raccomandazioni o pressioni provenienti da pubblici funzionari o incaricati di pubblico servizio ed accettare da questi regali, omaggi o altre utilità;
  - iv) presentare dichiarazioni non veritiere esibendo documenti in tutto o in parte non corrispondenti alla realtà od omettendo l'esibizione di documenti veri;
  - v) tenere condotte ingannevoli nei confronti delle P.A. tali da indurre queste ultime in errori di valutazione nel corso dell'analisi di richieste di autorizzazioni e simili.
- ***Gestione della selezione ed assunzione del personale e del sistema premiante.***

L'attività di gestione sia della selezione che delle assunzioni del personale potrebbe presentare profili di rischio in relazione ai delitti contro la Pubblica Amministrazione qualora la Società assumesse una nuova risorsa, indicata o comunque "vicina" a un pubblico ufficiale o incaricato di pubblico servizio, al fine di compiere un'azione corruttiva o comunque ottenere trattamenti di favore nell'ambito delle responsabilità del funzionario pubblico.

La gestione del sistema premiante potrebbe presentare profili di rischio inerenti i delitti contro la Pubblica Amministrazione qualora la Società eroghi ad una risorsa premi/incentivi in denaro, volutamente non proporzionati al proprio ruolo/competenze al fine di dotare il dipendente di una provvista per compiere azioni corruttive nei confronti di funzionari pubblici.

Ai Destinatari coinvolti nella selezione, assunzione e gestione del personale e nella gestione del sistema premiante è fatto obbligo di:

- i) operare nel rispetto del Codice Etico;
- ii) effettuare attività di selezione atte a garantire che la scelta dei candidati sia effettuata sulla base di considerazioni oggettive delle caratteristiche professionali e personali necessarie all'esecuzione del lavoro da svolgere evitando favoritismi di ogni sorta;
- iii) operare nel rispetto del criterio di meritocrazia e delle pari opportunità, senza nessuna discriminazione basata sul sesso, l'origine razziale ed etnica, la nazionalità, l'età, le opinioni politiche, le credenze religiose, lo stato di salute, l'orientamento sessuale, le condizioni economico-sociali, in relazione alle reali esigenze della Società;
- iv) assumere personale solo ed esclusivamente con regolare contratto di lavoro;
- v) garantire l'esistenza della documentazione attestante il corretto svolgimento delle procedure di selezione e assunzione;

## DIGITAL SOLUTIONS

- vi) curare che siano assicurate all'interno delle Società condizioni di lavoro rispettose della dignità personale, delle pari opportunità e un ambiente adeguato, nel rispetto della normativa contrattuale collettiva del settore e della normativa previdenziale, fiscale ed assicurativa;
- vii) assicurare che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti assegnati;
- viii) verificare che, con riferimento all'assunzione di cittadini di paesi terzi, gli stessi:
  - siano in possesso di permesso di soggiorno non scaduto o revocato o annullato;
  - in caso di permesso di soggiorno scaduto, sia stata presentata richiesta di rinnovo entro il termine previsto dalla normativa.

Nell'ambito dei citati comportamenti è fatto divieto di:

- i) operare secondo logiche di favoritismo;
  - ii) assumere personale, anche per contratti temporanei, senza il rispetto delle normative vigenti (ad esempio in termini di contributi previdenziali ed assistenziali, permessi di soggiorno, etc.);
  - iii) tollerare forme di lavoro irregolare o minorile o di sfruttamento della manodopera;
  - iv) assumere o promettere l'assunzione ad impiegati della Pubblica Amministrazione (o loro parenti, affini, amici, etc.) che abbiano partecipato a processi autorizzativi della Pubblica Amministrazione o ad atti ispettivi, nei confronti della Società;
  - v) promettere o concedere promesse di assunzione/avanzamento di carriera a risorse vicine o gradite a funzionari pubblici quando questo non sia conforme alle reali esigenze dell'azienda e non rispetti il principio della meritocrazia.
- ***Gestione del contenzioso e dei rapporti con l'Autorità giudiziaria e ispezioni.***

L'attività di gestione del contenzioso manifesta profili di rischio legati alla fattispecie di reato di corruzione in atti giudiziari (sia direttamente che per il tramite di consulenti legali) in occasione dei rapporti con l'Autorità Amministrativa e Giudiziaria, al fine di favorire la Società in processi pur in assenza dei presupposti.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione del contenzioso è fatto obbligo di:

- i) prevedere che i contratti con i legali e tutti gli atti siano firmati dal legale rappresentante o dai soggetti dotati di specifica procura;
- ii) garantire che tutta la documentazione in materia di contenzioso sia archiviata dalle funzioni coinvolte nel processo.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione del contenzioso è fatto divieto di:

- i) effettuare prestazioni o pagamenti in favore di legali esterni, consulenti, periti o altri soggetti terzi che operino per conto della Società nell'ambito delle attività disciplinate dal presente protocollo, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;

## DIGITAL SOLUTIONS

- ii) adottare comportamenti contrari alle leggi e al Codice Etico in sede di incontri formali ed informali, anche a mezzo di legali esterni e Consulenti, per indurre giudici o membri di collegi arbitrali (compresi gli ausiliari e i periti d'ufficio) a favorire indebitamente gli interessi della Società;
- iii) adottare comportamenti contrari alle leggi e al Codice Etico in sede di ispezioni, controlli o verifiche da parte degli organismi pubblici o periti d'ufficio, per influenzarne il giudizio/parere nell'interesse della Società, anche a mezzo di legali esterni e consulenti.

La gestione dei rapporti con l'Autorità giudiziaria potrebbe presentare profili di rischio inerenti il reato di induzione e non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria nell'ipotesi in cui un dipendente imputato o indagato in un procedimento penale venga indotto a rendere false dichiarazioni (o ad astenersi dal renderle) per evitare un maggior coinvolgimento della Società stessa.

Nell'espletamento di tutte le operazioni attinenti alla gestione dei rapporti con l'Autorità giudiziaria, oltre al complesso di regole di cui al presente Modello, ai Destinatari è fatto obbligo di conoscere e rispettare quanto di seguito riportato:

- i) nei rapporti con l'Autorità giudiziaria, i Destinatari sono tenuti a prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaustivamente rappresentative dei fatti;
- ii) nei rapporti con l'Autorità giudiziaria, i Destinatari e, segnatamente, coloro i quali dovessero risultare indagati o imputati in un procedimento penale, anche connesso, inerente l'attività lavorativa prestata nella Società, sono tenuti ad esprimere liberamente le proprie rappresentazioni dei fatti od a esercitare la facoltà di non rispondere accordata dalla legge;
- iii) tutti i Destinatari devono tempestivamente avvertire, attraverso gli strumenti di comunicazione esistenti all'interno della Società (oppure con qualsivoglia strumento di comunicazione, purché nel rispetto del principio di tracciabilità), l'Organismo di Vigilanza di ogni atto, citazione a testimoniare e procedimento giudiziario (civile, penale o amministrativo) che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente. L'Organismo di Vigilanza può informarne il Responsabile dell'area legale o altri Responsabili della Società, nonché prendere parte agli incontri con i referenti aziendali e con i consulenti legali eventualmente coinvolti;
- iv) l'Organismo di Vigilanza deve poter ottenere una piena conoscenza del procedimento in corso, anche attraverso la partecipazione ad incontri inerenti i relativi procedimenti o comunque preparatori all'attività difensiva del Destinatario medesimo, anche nelle ipotesi in cui i predetti incontri prevedano la partecipazione di consulenti esterni.

Nell'ambito dei citati comportamenti è fatto divieto di:

- i) coartare od indurre, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse della Società, la volontà dei Destinatari di rispondere all'Autorità giudiziaria o di avvalersi della facoltà di non rispondere;
- ii) accettare, nei rapporti con l'Autorità giudiziaria, denaro o altra utilità, anche attraverso consulenti della Società medesima;
- iii) indurre il Destinatario, nei rapporti con l'Autorità giudiziaria, a rendere dichiarazioni non veritiere.

Alle ispezioni giudiziarie, tributarie e amministrative (quali, ad esempio, verifiche tributarie, verifiche NPS, etc.) devono partecipare i soggetti a ciò espressamente delegati o autorizzati. L'OdV dovrà essere prontamente informato di ogni attività ispettiva, mediante apposita comunicazione interna. Di tutto il procedimento relativo all'ispezione devono essere redatti gli apposti verbali.

- ***Gestione degli acquisti e delle consulenze.***

Ai Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione degli acquisti e delle consulenze è richiesto di:

- i) favorire, nei processi di acquisto, fornitori, consulenti che siano stati selezionati ed inseriti in apposito albo sulla base di criteri di valutazione oggettivi;
- ii) tracciare e motivare la scelta di fornitori e di consulenti che si discostino dai criteri *standard* e procedure di acquisto aziendali e ad a cui l'incarico professionale o la richiesta di fornitura venga stabilita sulla base di esigenze specifiche della Società;
- iii) prevedere apposite clausole contrattuali con i quali debbano essere rispettati il Modello, i principi in esso contenuti e/o il Decreto, prevedendo, in caso di violazione, una sanzione contrattuale graduata a seconda della violazione commessa (risoluzione del rapporto, clausola penale).

**PARTE SPECIALE B**

**REATI SOCIETARI**

**Articolo 25-ter del Decreto Legislativo 231/2001**

## DIGITAL SOLUTIONS

### B.1. Funzione della Parte Speciale B.

La presente Parte Speciale si riferisce ai c.d. reati societari, il cui obiettivo è quello di indicare le regole di condotta necessarie al fine di non commettere i Reati meglio identificati all'articolo 25-ter del Decreto.

Nello specifico la presente Parte Speciale ha lo scopo di:

- a) definire le procedure che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- b) fornire ai responsabili delle funzioni interne quali gli Organi Sociali o soggetti che cooperano con tali funzioni, nonché all'OdV, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

### B.2. Fattispecie di Reato rilevanti.

Si provvede qui di seguito a fornire una breve descrizione dei Reati ivi contemplati, così come indicati all'articolo 25-ter del Decreto (di seguito i “**Reati Societari**”).

#### B.2.2. Reati Societari.

*Le ipotesi di falsità.*

##### **False comunicazioni sociali (articolo 2621 del Codice Civile).**

Le false comunicazioni sono costituite dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Società in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionando un danno patrimoniale alla società, ai soci o ai creditori. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

##### **Fatti di lieve entità (articolo 2621-bis del Codice Civile).**

La fattispecie si colloca nel novero delle circostanze attenuanti. La norma, infatti, nulla aggiunge e nulla toglie rispetto al precetto contenuto all'interno del richiamato articolo 2621 del Codice Civile, limitandosi a determinare una diminuzione di pena nel caso in cui i fatti ivi contemplati siano di lieve entità, tenuto conto della natura e delle dimensioni della Società e delle modalità o degli effetti della condotta.

##### **False comunicazioni sociali in danno della società quotate (articolo 2622 del Codice Civile).**

Riguarda la condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico ed al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero omettendo informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Società, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione e

anche ponendo in essere azioni in concorso alla realizzazione delle attività di cui sopra che configurano la fattispecie di reato in oggetto, cagionano un danno patrimoniale ai soci o ai creditori.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla Società per conto di terzi.

### **Omessa comunicazione del conflitto di interessi (articolo 2629-bis del Codice Civile).**

Il reato in esame si configura allorché un componente del consiglio di amministrazione o del consiglio di gestione di una società - con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al Decreto Legislativo 24 febbraio 1998, n. 58, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al Decreto Legislativo n. 58 del 1998, della Legge 12 agosto 1982, n. 576, o del Decreto Legislativo 21 aprile 1993, n. 124 - violando la disciplina in materia di interessi degli amministratori prevista dal codice civile, rechi alla stessa o a terzi un danno.

Più in specifico, la norma rimanda all'articolo 2391 primo comma, del Codice Civile, che impone ai membri del consiglio di amministrazione di comunicare (agli altri membri del consiglio e ai sindaci) ogni interesse che i medesimi, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata.

*La tutela del capitale sociale.*

### **Indebita restituzione dei conferimenti (articolo 2626 del Codice Civile).**

Il reato in questione, come quello previsto dal successivo articolo 2627 del Codice Civile, riguarda la tutela dell'integrità del capitale sociale e si compie quando gli amministratori, in assenza di legittime ipotesi di riduzione del capitale sociale, provvedono a restituire, anche per equivalente, i conferimenti effettuati dai soci ovvero liberano i soci dall'obbligo di eseguirli.

Il reato in esame assume rilievo solo quando, per effetto degli atti compiuti dagli amministratori, si intacca il capitale sociale e non i fondi o le riserve. Per questi ultimi, eventualmente, sarà applicabile il reato contemplato dal successivo articolo 2627 del Codice Civile.

La restituzione dei conferimenti può essere palese (quando gli amministratori restituiscono beni ai soci senza incasso di alcun corrispettivo o rilasciano dichiarazioni dirette a liberare i soci dai loro obblighi di versamento) ovvero, più probabilmente, simulata (quando per realizzare il loro scopo gli amministratori utilizzano stratagemmi o artifici quali, per esempio, la distribuzione di utili fittizi con somme prelevate dal capitale sociale e non dalle riserve, oppure la compensazione del credito vantato dalla società con crediti inesistenti vantati da uno o più soci).

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

### **Illegale ripartizione di utili e riserve (articolo 2627 del Codice Civile).**

Il reato riguarda la condotta degli amministratori, i quali ripartiscono utili, o acconti sugli utili, che non sono stati effettivamente conseguiti, o che sono destinati per legge a riserva.

La fattispecie potrebbe verificarsi inoltre attraverso la ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite.

### **Indebita ripartizione di beni sociali da parte dei liquidatori (articolo 2633 del Codice Civile).**

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, che cagioni un danno ai creditori. Soggetti attivi sono i liquidatori e costituisce una modalità di estinzione del reato il risarcimento del danno ai creditori prima del giudizio.

### **Illecite operazioni sulle azioni o quote sociali o della società controllante (articolo 2628 del Codice Civile).**

Il reato è costituito dalla condotta degli amministratori mediante l'acquisto o la sottoscrizione, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della società controllante in modo tale da procurare una lesione all'integrità del capitale sociale e delle riserve non distribuibili per legge.

### **Operazioni in pregiudizio dei creditori (articolo 2629 del Codice Civile).**

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Il reato è punibile a querela di parte ed i soggetti attivi del reato sono, anche in questo caso, gli amministratori.

### **Formazione fittizia del capitale (articolo 2632 del Codice Civile).**

Il reato riguarda la condotta degli amministratori e dei soci conferenti i quali, anche in parte, formano o aumentano in modo fittizio il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

*La tutela del corretto funzionamento della società.*

### **Impedito controllo (articolo 2625 del Codice Civile).**

Il reato di impedito controllo si verifica nell'ipotesi in cui, attraverso l'occultamento di documenti o altri idonei artifici, si impedisca o semplicemente si ostacoli lo svolgimento delle attività di controllo legalmente attribuite ai soci e ad altri organi sociali<sup>4</sup>.

Il reato si considera imputabile alla società unicamente nell'ipotesi in cui l'impedimento, o il semplice ostacolo abbia cagionato un danno ai soci, stante l'esplicito riferimento al solo secondo comma di tale disposizione, contenuto nel Decreto Legislativo 231/2001.

---

<sup>4</sup>Così come modificato dall'articolo 37 comma 35 lettera a) del Decreto Legislativo 39/2010. La nuova fattispecie di impedito controllo alle società di revisione è disciplinata dall'art 29 del Decreto Legislativo 39/2010 non espressamente richiamato dal Decreto Legislativo 231/2001.



### **Illecita influenza sull'assemblea (articolo 2636 del Codice Civile).**

Il reato si perfeziona quando chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

È opportuno ricordare che la responsabilità dell'ente è configurabile solo quando la condotta prevista dall'articolo in esame sia realizzata nell'interesse dell'ente. Pertanto nel caso di specie l'ipotesi di coinvolgimento della società è remoto dato che di norma, l'illecita influenza sull'assemblea viene realizzata per favorire interessi di parte e non dell'"ente".

*La tutela penale contro le frodi.*

### **Aggiotaggio (articolo 2637 del Codice Civile).**

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

*La tutela delle funzioni di vigilanza.*

### **Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (articolo 2638 del Codice Civile).**

Il reato si realizza nel caso in cui determinati soggetti (amministratori, direttori generali, sindaci, liquidatori di società o enti e, in generale, i soggetti sottoposti alle autorità pubbliche di vigilanza *ex lege*) esponano, in occasione di comunicazioni alle autorità pubbliche di vigilanza, cui sono tenuti in forza di legge, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che erano tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi. In tale ipotesi il reato si perfeziona nel caso in cui la condotta criminosa sia specificamente volta ad ostacolare l'attività delle autorità pubbliche di vigilanza.

Il reato si realizza, altresì, indipendentemente dal fine perseguito dagli stessi soggetti, ma soltanto qualora l'attività dell'autorità di pubblica vigilanza sia effettivamente ostacolata dalla loro dei predetti soggetti, di qualunque genere essa sia, anche omissiva.

### **B. 3. Aree a Rischio ed Attività Sensibili.**

Di seguito sono elencate le attività che, per il loro contenuto intrinseco, nell'ambito delle Aree a Rischio quali amministrazione, contabilità, bilancio ed affari societari sono considerate maggiormente esposte alla commissione dei Reati di cui al Decreto:

- *Predisposizione del bilancio e gestione della fiscalità, tenuta della documentazione, rapporti con il collegio sindacale e società di revisione;*
- *Gestione delle attività assembleari e operazioni societarie che possono incidere sull'integrità del capitale sociale;*
- *Comunicazioni sociali previste dalla legge dirette ai soci ed al pubblico (i.e. informazioni relative ai bilanci e relazioni riguardanti la situazione economica, patrimoniale e finanziaria della società).*

## DIGITAL SOLUTIONS

- *Gestione dei rapporti con gli Organi Sociali e di controllo.*

### B.4. Principi generali di comportamento.

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari come sopra definiti.

Nell'espletamento di tutte le operazioni attinenti alla gestione della Società, oltre alle regole di cui al presente Modello ed, in particolare, a quelle indicate al successivo paragrafo i Destinatari devono in generale conoscere e rispettare:

- i) i principi di *corporate governance* e le *best practice* per una corretta gestione della struttura organizzativa e dell'attività imprenditoriale;
- ii) le procedure interne della Società, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale ed organizzativa ed il sistema di controllo della gestione;
- iii) le norme inerenti il sistema amministrativo, contabile, finanziario e di *reporting*;
- iv) in generale, la normativa applicabile.

In particolare, i Destinatari, nei limiti delle competenze e della partecipazione alle Attività Sensibili considerate della presente Parte Speciale, dovranno attenersi ai seguenti principi di condotta:

- i) astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati Societari.
- ii) astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.
- iii) tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai propri soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società. In ordine a tale punto, è fatto divieto di:
  - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;
  - omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
  - non attenersi ai principi e alle prescrizioni contenute nelle istruzioni predisposte o applicate dalla Società per la redazione dei bilanci;
- iv) osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale ed 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 al riguardo. In ordine a tale punto, è fatto divieto di:

- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
  - porre in essere azioni finalizzate a fornire informazioni fuorvianti con riferimento all'effettiva rappresentazione della Società, non fornendo una corretta rappresentazione della situazione economica, patrimoniale e finanziaria della Società;
  - restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale
  - ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
  - acquistare o sottoscrivere azioni della Società o dell'eventuale società controllante fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge;
  - effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
  - procedere in ogni modo a formazione o aumento fittizi del capitale sociale;
  - ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli
  - presentare dichiarazioni non veritiere alle Autorità di Vigilanza, esibendo documenti in tutto o in parte non corrispondenti alla realtà;
- v) assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare. In ordine a tale punto, è fatto divieto di:
- tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della società di revisione o dei soci;
  - porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

### **B.5. Principi specifici di comportamento.**

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del Modello, gli specifici principi procedurali qui di seguito descritti.

- ***Predisposizione del bilancio e gestione della fiscalità, tenuta della documentazione, rapporti con il Collegio Sindacale e società di revisione.***

## DIGITAL SOLUTIONS

Le attività connesse alla predisposizione del bilancio e alla gestione della fiscalità potrebbero presentare profili di rischio in relazione alla commissione del reato di false comunicazioni sociali ad esempio attraverso l'approvazione di un bilancio non veritiero anche a causa di una non corretta gestione, registrazione, aggregazione e valutazione dei dati contabili, ovvero attraverso l'esposizione nella nota integrativa di fatti materiali non rispondenti al vero o in caso di omissione o alterazione di informazioni sulla situazione economica, patrimoniale o finanziaria al fine di indurre in errore i destinatari quali il Collegio Sindacale, i soci, gli amministratori non esecutivi e terzi in genere.

L'attività potrebbe presentare altresì profili di rischio in relazione al reato di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza nell'ipotesi in cui, ad esempio, gli amministratori esponano, in occasione di comunicazioni alle autorità pubbliche di vigilanza cui sono tenuti in forza di legge, fatti materiali non rispondenti al vero al fine di ostacolarne l'attività.

Inoltre, la Società potrebbe incorrere nel rischio di impedito controllo ai soci, indebita restituzione dei conferimenti ai soci, illegale ripartizione di utili e riserve, illecite operazioni sulle azioni o quote sociali e operazioni in pregiudizio dei creditori e formazione fittizia del capitale.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione della contabilità generale e nella predisposizione del bilancio d'esercizio e dei relativi allegati è fatto obbligo di:

- i) tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge, dei principi contabili applicabili e delle procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale, finanziaria e fiscale della Società;
- ii) osservare le regole di chiara, corretta e completa registrazione nell'attività di contabilizzazione dei fatti relativi alla gestione della Società;
- iii) procedere alla valutazione e registrazione di elementi economico patrimoniali 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;
- iv) assicurare il rispetto delle regole di segregazione dei compiti tra il soggetto che ha effettuato l'operazione, chi provvede alla registrazione in contabilità e chi ad effettuare il relativo controllo;
- v) osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- vi) gestire in maniera corretta e sufficientemente dettagliata documenti, relazioni e altre annotazioni, mantenendo documentazione delle attività e garantendone la sua conservazione tramite corretta archiviazione e segregazione;
- vii) improntare i rapporti con le Autorità di Vigilanza, nel caso di specie che si occupino di profili economici/fiscali, alla massima trasparenza, collaborazione, disponibilità e nel pieno rispetto del ruolo istituzionale rivestito da esse e delle previsioni di legge esistenti in materia, dei principi generali e delle regole di comportamento richiamate nel Codice Etico nonché nella presente Parte Speciale e nella Parte Speciale relativa ai rapporti con la PA. I Destinatari devono pertanto dare sollecita esecuzione alle prescrizioni delle medesime Autorità ed agli adempimenti richiesti;

## DIGITAL SOLUTIONS

- viii) gestire gli adempimenti nei confronti della Pubblica Amministrazione e delle Autorità di Vigilanza, nonché la predisposizione della relativa documentazione nel rispetto delle previsioni di legge esistenti in materia e dei principi generali e delle regole di comportamento richiamate nel Codice Etico e nella presente Parte Speciale;
  - ix) effettuare ogni adempimento connesso al proprio ruolo, con la massima diligenza e professionalità, in modo da generare informazioni chiare, accurate, complete, fedeli e veritiere, ed evitare situazioni di conflitto di interesse;
  - x) assicurare che gli adempimenti fiscali siano eseguiti o supportati da professionisti qualificati e che la documentazione trasmessa sia prodotta dalle persone competenti in materia e preventivamente identificate;
  - xi) effettuare tempestivamente e correttamente, in modo veridico e completo, le comunicazioni previste dalla legge, dai regolamenti e dalle norme aziendali nel tempo vigenti nei confronti delle autorità o organi di vigilanza o controllo, del mercato o dei soci.
- ***Gestione delle attività assembleari e operazioni societarie che possono incidere sull'integrità del capitale sociale.***

La gestione delle attività assembleari potrebbe presentare profili di rischio in relazione alla commissione del reato di influenza illecita sull'assemblea, nel caso in cui la maggioranza in assemblea dovesse in qualsiasi modo essere raggiunta attraverso atti simulati o fraudolenti, ad esempio attraverso la presentazione di documenti o informazioni false o fuorvianti.

Le operazioni sul capitale potrebbero presentare profili di rischio in relazione alla commissione dei reati di indebita restituzione dei conferimenti, illegale ripartizione di utili o riserve, illecite operazioni sulle azioni o quote sociali e formazione fittizia del capitale qualora gli amministratori e/o i soci compiano operazioni illecite che vanno a intaccare il patrimonio della Società.

I soggetti coinvolti dovranno assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo e agevolando la libera e corretta formazione della volontà assembleare.

In particolare, la funzione preposta alla gestione della segreteria societaria ha il compito di predisporre, nel rispetto delle norme di legge e di statuto, delle procedure operative di controllo sulle fasi di:

- i) regolare convocazione dell'assemblea;
- ii) deposito di ogni documento idoneo all'assunzione delle delibere da parte dei soci;
- iii) regolare esercizio del diritto di voto.

Con riferimento a operazioni di finanza straordinaria (riferite tipicamente a assunzione di mutui e finanziamenti, sottoscrizione e aumenti di capitale sociale, concessione di garanzie e fidejussioni, concessione di finanziamenti e sottoscrizione di obbligazioni, acquisizioni di rami d'azienda o partecipazioni azionarie, altre operazioni straordinarie quali fusioni, scissioni, conferimenti) i soggetti coinvolti dovranno assicurare: che il soggetto competente, sia esso l'Amministratore Delegato, il Consiglio di Amministrazione o altra persona formalmente delegata, disponga di un supporto informativo adeguato tale da poter esprimere una decisione consapevole.

La funzione delegata ovvero il comitato incaricato della gestione di tale attività sono tenuti, per ogni operazione di finanza straordinaria da deliberare, alla preparazione della documentazione idonea a valutarne la fattibilità e la convenienza strategica e economica, comprendente, ove applicabile.

## DIGITAL SOLUTIONS

- ***Comunicazioni sociali previste dalla legge dirette ai soci ed al pubblico (i.e. informazioni relative ai bilanci e relazioni riguardanti la situazione economica, patrimoniale e finanziaria della Società).***

La gestione delle attività relative alle comunicazioni sociali presenta remoti profili di rischio con riferimento a Digital Solutions. Ad ogni modo è stato valutato il potenziale rischio in cui le comunicazioni sociali abbiano contenuti non veritieri o fuorvianti.

Le suddette comunicazioni, pertanto, devono essere costruite e redatte con chiarezza e completezza affinché vengano presentate e condivise informazioni veritiere riguardo lo stato della Società.

A tal proposito la Società si è dotata di procedure formali che:

- i) disciplinino i comportamenti da tenere nella gestione delle comunicazioni verso l'esterno;
- ii) individuare, nell'ambito dell'organizzazione aziendale, i soggetti che sono autorizzati a divulgare informazioni al pubblico relative all'azienda;
- iii) disciplinare in modo puntuale i rapporti con i media.

- ***Gestione dei rapporti con gli Organi Sociali e di controllo.***

Nei rapporti tra la Società e la società di revisione contabile sono adottati i seguenti presidi:

- i) rispetto delle fasi di valutazione e selezione della società di revisione contabile;
- ii) gli incarichi, diversi da quelle del bilancio d'esercizio e di revisione contabile, purché consentiti dalla legge e dai regolamenti, vengono conferiti alla società di revisione, previo parere del Collegio Sindacale;
- iii) rispetto delle disposizioni normative e statutarie relative ai rapporti tra Organi Sociali nonché attraverso la tenuta e conservazione ordinata e correttamente segregata di tutta la documentazione attinente all'attività aziendale.

**PARTE SPECIALE C**

**REATI DI CORRUZIONE TRA PRIVATI ED  
ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI**

**Articolo 25-ter del Decreto Legislativo 231/2001**

## DIGITAL SOLUTIONS

### C.1. Funzione della Parte Speciale C.

La presente Parte Speciale si riferisce ai comportamenti posti in essere dai Dipendenti, dai componenti degli Organi Sociali, da Consulenti, *Partner* e Terzi come già definiti nella Parte Generale.

L'obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati adottino regole di condotta conformi a quanto prescritto nella stessa.

Nello specifico la presente Parte Speciale ha lo scopo di:

- a) indicare le procedure che i Destinatari sono chiamati ad osservare al fine di applicare correttamente le prescrizioni del Modello;
- b) fornire ai responsabili delle funzioni interne quali gli Organi Sociali o soggetti che cooperano con tali funzioni, nonché all'OdV, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

### C.2. Fattispecie di Reato rilevanti.

#### C.2.1. Fattispecie di “*corruzione tra privati*” e “*istigazione alla corruzione tra privati*”.

La presente Parte Speciale si riferisce ai reati di “*corruzione tra privati*”, di cui all'articolo 2635 del Codice Civile, e di “*istigazione alla corruzione tra privati*” di cui all'articolo 2635-bis del Codice Civile, rispettivamente introdotti nel *corpus* del Decreto Legislativo 231/2001 all'articolo 25-ter, comma 1, lettera s)-bis dalla Legge 6 novembre 2012, n. 160 (c.d. “*Legge Anticorruzione*”) e dal Decreto Legislativo 15 marzo 2017, n. 38, il quale ha altresì riformulato il reato di “*corruzione tra privati*”.

Sebbene i suddetti Reati siano ricompresi dal Decreto tra i c.d. Reati Societari, Digital Solutions ha deciso di adottare un capitolo *ad hoc* in considerazione della peculiarità di tali fattispecie di Reato, della tipologia di attività rientranti tra le Aree a Rischio e della volontà di creare un idoneo sistema di controllo volto a presidiarle.

#### **Corruzione tra Privati (articolo 2635 del Codice Civile).**

Tale ipotesi di Reato è contemplata nel novero dei Reati Presupposto esclusivamente per quanto riguarda la condotta “attiva” del corruttore (e non anche dunque con riferimento alla condotta del soggetto corrotto). Saranno in tal senso rilevanti ai fini dell'applicabilità della responsabilità amministrativa ai sensi del Decreto le condotte di coloro che, anche per interposta persona, diano o promettano o offrano denaro o altra utilità non dovuti ad uno dei seguenti soggetti (in quanto appartenente ad una società o altro ente privato):

- i) un amministratore;
- ii) un direttore generale (se esistente);
- iii) un dirigente preposto alla redazione dei documenti contabili (se esistente);
- iv) un sindaco;
- v) un liquidatore;
- vi) altro soggetto che eserciti funzioni direttive diverse da quelle dei soggetti indicati sopra; o



vii) qualsiasi sottoposto alla direzione o vigilanza di uno dei soggetti di cui ai precedenti punti.

La dazione o la promessa di denaro deve essere volta al compimento o all'omissione, da parte del soggetto corrotto, di un atto in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà nei confronti della società o ente privato di appartenenza.

Si segnala infine che il Reato è perseguibile a querela della parte offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

L'eliminazione del riferimento al "*documento alla società*" – prima della modifica di cui al Decreto Legislativo 15 marzo 2017, n. 38 presupposto necessario della configurabilità del reato – comporta un'anticipazione del momento consumativo e pone l'accento non più sul danno subito dall'ente in seguito alla condotta delittuosa dell'agente, ma sulla violazione da parte di quest'ultimo degli obblighi di ufficio o di fedeltà.

### **Istigazione alla corruzione tra privati (articolo 2635-*bis* del Codice Civile).**

L'articolo 2635-*bis* del Codice Civile primo comma - ricompreso nel novero dei reati presupposto - comporta la punibilità ai sensi del Decreto anche della condotta di colui che offre o promette denaro o altra utilità non dovuti a uno dei soggetti menzionati al paragrafo che precede (e per i fini illeciti ivi indicati) quando l'offerta o la promessa non sia accettata.

Il momento consumativo del reato viene dunque anticipato alla mera promessa o offerta anche laddove questa non trovi seguito per mancata accettazione del destinatario (andando di fatto a costituire una fattispecie del tutto simile al tentativo).

\*\*\*

Per quanto riguarda le sanzioni applicabili agli enti nell'ipotesi di commissione dei Reati di corruzione tra privati, possono consistere in sanzioni di natura pecuniaria da un minimo di duecento quote fino ad un massimo di seicento quote nonché in sanzioni interdittive (tra quelle previste dal Decreto).

### **C.3. Aree di Rischio e Attività Sensibili.**

Tenuto conto dell'approccio metodologico adottato recentemente dalla Società, volto a migliorare i presidi aziendali, e la grande rilevanza che si è voluto dare ai reati di corruzione, nel presente capitolo sono state identificate sia le Area a Rischio, sia delle Attività Sensibili (ovvero le attività strumentali) rilevate con riferimento alle varie divisioni/funzioni aziendali.

Pertanto, in relazione ai Reati e alle condotte criminose meglio esplicitate al capitolo precedente, le aree ritenute più specificamente a rischio risultano essere le seguenti:

- ***Gestione dell'amministrazione ed assunzione del personale.***
  - i) definizione del piano di assunzioni sulla base del fabbisogno di risorse umane in relazione agli obiettivi strategici e reale necessità indicata dai soggetti responsabili delle varie funzioni aziendali;
  - ii) gestione del processo di selezione del personale (dipendenti e *stage*), inclusi la raccolta delle candidature ed il reclutamento dei candidati;
  - iii) definizione degli obiettivi e valutazione delle performance del personale;

## DIGITAL SOLUTIONS

- iv) gestione amministrativa del personale dipendente e somministrato;
- v) regolamentazione delle trasferte e dei rimborsi spesa.
- ***Gestione dell'amministrazione, contabilità e bilancio.***
  - i) gestione anagrafiche;
  - ii) registrazioni di contabilità generale: emissione e contabilizzazione fatture passive e attive;
  - iii) verifica della corrispondenza tra il bene/servizio ricevuto e quanto inserito nella fattura;
  - iv) gestione del credito: verifica dello stato dei crediti e del pagamento delle relative fatture e attività di sollecito dei pagamenti.
- ***Gestione della Tesoreria.***
  - i) verifica della corrispondenza e gestione del credito come al punti iii) e iv) che precedono ;
  - ii) apertura e/o chiusura e gestione dei c/c bancari e gestione rapporti con le banche;
  - iii) gestione dei flussi di cassa, verifica e registrazione degli incassi;
  - iv) predisposizione e registrazione dei pagamenti;
  - v) gestione delle carte di credito aziendali.
- ***Selezione e gestione acquisti di beni, consulenze e servizi.***
  - i) definizione del fabbisogno di acquisto ed emissione di richieste di acquisto;
  - ii) emissione ordini e stipula di contratti;
  - iii) monitoraggio dell'attività dei fornitori;
  - iv) qualifica e selezione e gestione dei fornitori.
- ***Gestione delle vendite e delle commesse.***
  - i) definizione e applicazione di politiche commerciali (come ad esempio prezzi, scontistica, etc.);
  - ii) raccolta delle richieste di offerta;
  - iii) valutazione preventiva dell'affidabilità del cliente;
  - iv) predisposizione dell'offerta tecnica/economica;
  - v) gestione dell'attività di negoziazione, stipula ed acquisizione degli ordini dal cliente.
- ***Partecipazione e gestione di bandi di gara.***

## DIGITAL SOLUTIONS

- i) partecipazione a procedure di gara o di negoziazione diretta indette da enti pubblici o privati italiani o stranieri per l'assegnazione di commesse (di appalto, di fornitura o di servizi);
- ii) gestione dei rapporti di *partnership* (raggruppamenti temporanei di impresa);
- iii) predisposizione dell'offerta tecnica/economica.

- ***Gestione dei flussi finanziari***

La gestione dei flussi finanziari potrebbe presentare profili di rischio in relazione ai reati qui menzionati qualora un soggetto apicale o sottoposto di Digital Solutions distraiga ed utilizzi le risorse finanziarie della Società per commettere azioni corruttive.

Nella gestione dei flussi finanziari la Società deve prevedere:

- i) che siano autorizzati alla gestione ed alla movimentazione dei flussi finanziari solo soggetti dotati di apposita procura;
- ii) che siano fissati limiti all'utilizzo autonomo delle risorse finanziarie, mediante la definizione di soglie quantitative coerenti con i ruoli e le responsabilità organizzative attribuite alle singole persone;
- iii) che tutti i pagamenti siano effettuati a fronte di fatture gestite a sistema con i relativi ordini e comunque approvate dalla funzione richiedente che ne attesta l'avvenuta prestazione e conseguentemente autorizza il pagamento;
- iv) che, per prassi, non siano consentiti pagamenti per contanti, ad eccezione di quelli di valore non significativo (valori bollati etc.) e comunque nei limiti previsti dalla normativa;
- v) che tutti le movimentazioni di flussi finanziari siano effettuate con strumenti tracciabili.

Ai Destinatari a qualsiasi titolo coinvolti nelle Aree a Rischio sopra individuate è fatto obbligo di:

- i) operare nel rispetto dei principi espressi nel Codice Etico, del Modello e della normativa vigente;
- ii) garantire la tracciabilità delle fasi del processo decisionale relativo ai rapporti finanziari con soggetti terzi, attraverso l'informativa periodica all'Amministratore Delegato nonché l'archiviazione della documentazione rilevante a supporto delle transazioni;
- iii) assicurare che tutte le disposizioni sui conti correnti bancari intestati alla Società, nonché i pagamenti eseguiti con modalità differenti (ad es. assegni non trasferibili, carte di credito aziendali), siano adeguatamente documentate ed autorizzate secondo il sistema di deleghe e procure in vigore.

Nell'ambito dei citati comportamenti è fatto divieto di:

- i) effettuare pagamenti per contanti o con mezzi di pagamento non tracciabili;
- ii) effettuare pagamenti non adeguatamente documentati;
- iii) creare fondi a fronte di pagamenti non giustificati (in tutto o in parte).

- ***Gestione dei rapporti con società di certificazione e con il revisore***

Per la gestione dei rapporti con le società di certificazione e società di revisione, si rimanda ai principi generali riportati nella Parte Speciale B per quanto riguarda la regolare tenuta delle scritture contabili nonché riguardo le comunicazioni sociali ponendo il divieto ai Destinatari di tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o del revisore o dei soci nonché degli enti certificatori.

### C.4 Regole e principi generali di comportamento.

Obiettivo del presente capitolo è che i Destinatari si attengano, nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento delle Attività Sensibili individuate in precedenza, a regole di condotta conformi.

In particolare, i Destinatari, nei limiti delle competenze e della partecipazione alle Attività Sensibili considerate nella presente Parte Speciale, dovranno attenersi ai seguenti principi di condotta:

- i) astenersi dal tenere comportamenti tali da integrare il Reato di corruzione tra privati;
- ii) astenersi dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi del Reato suddetto, possano potenzialmente diventarlo;
- iii) astenersi dal porre in essere situazioni che inducano un soggetto che agisca per conto di una società - con cui Digital Solutions entri direttamente o indirettamente in relazione - ad anteporre il proprio interesse personale a quello sociale, dando luogo a situazioni di conflitto.

A tal proposito, ai Destinatari è fatto assoluto divieto di:

- i) offrire o promettere a terzi denaro o altre liberalità con l'intento di acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società. In particolare, è vietata ogni forma di liberalità verso qualsiasi controparte, italiana o straniera (anche in quei Paesi dove l'elargizione di liberalità rappresenta una prassi accettata e diffusa), che possa indurre la stessa ad accordare un qualsiasi vantaggio alla Società o comunque influenzarne l'indipendenza di giudizio. A titolo esemplificativo, deve considerarsi come idonea ad influenzare l'indipendenza di giudizio della controparte: la liberalità, la cui natura o il cui valore esulino dalle normali pratiche di cortesia vigenti in ambito locale, offerta ad una persona (o ad un suo prossimo) che abbia recentemente assunto o debba assumere a breve una decisione riguardante l'attività della Società;
- ii) offrire o promettere un vantaggio di qualsiasi natura verso una controparte italiana o straniera (es. promessa di assunzione di un parente) che possa determinare gli stessi effetti di cui al punto che precede;
- iii) riconoscere compensi o effettuare prestazioni in favore di Consulenti, Fornitori o *Partner* che non trovino adeguata giustificazione rispettivamente all'incarico da svolgere, al tipo di prestazione richiesta, caratteristiche del rapporto di *partnership* e prassi vigenti in ambito locale.

### C.5 Principi specifici di comportamento.

Ai fini del rispetto dei principi e delle regole generali, nonché dei divieti elencati al precedente Capitolo, Digital Solutions adotta, con riferimento alle singole Aree a Rischio, specifici principi procedurali qui di seguito descritti.

- ***Con riferimento alla gestione delle vendite e delle commesse, la Società adotta procedure aziendali che prevedono:***
  - i) specifici limiti al potere negoziale del personale addetto alla vendita dei beni e servizi promossi da Digital Solutions (*es.* definizione dei prezzi e delle scontistica, etc.) e controlli sull'effettivo rispetto degli stessi;
  - ii) il coinvolgimento di più esponenti aziendali nelle diverse fasi di acquisizione e gestione delle commesse;
  - iii) la trasparenza e la tracciabilità del processo di acquisizione e gestione delle commesse;
  - iv) l'esecuzione di preventivi controlli, verifiche ed accertamenti, il cui grado di accuratezza deve essere valutato in ragione della tipologia di attività, del Paese di riferimento e del grado di conoscenza già acquisito sulla controparte, volte ad accertare l'affidabilità e la reputazione del cliente.
  
- ***Con riferimento alla selezione e gestione acquisti di beni, consulenze e servizi, la Società adotta procedure aziendali che prevedono:***
  - i) la segregazione dei ruoli relativi alla richiesta e assegnazione degli incarichi;
  - ii) la valutazione comparativa di più offerte contrattuali da parte di Consulenti e Fornitori diversi, salvo deroghe disciplinate da apposite procedure aziendali o da apposite delibere del CdA ovvero di disposizione dell'AD;
  - iii) la formalizzazione, da parte dell'unità richiedente, dell'esigenza della consulenza o dell'acquisto richiesti;
  - iv) la verifica, da parte dell'unità emittente, della congruità dei corrispettivi negoziati;
  - v) la forma scritta dell'accordo e l'indicazione nello stesso del compenso pattuito o delle modalità con cui determinare lo stesso;
  - vi) la verifica dell'effettiva esecuzione dell'incarico da parte dell'unità richiedente;
  - vii) l'adozione di modalità di pagamento che escludano l'utilizzo di conti non intestati al consulente/fornitore e, in ogni caso, escludano pagamenti in contanti;
  - viii) la predisposizione di apposite liste di Consulenti e di Fornitori già qualificati (*i.e.* albo fornitori);
  - ix) l'inserimento nei contratti di clausole che impegnino i Consulenti e i Fornitori, nella conduzione dei propri affari e nella gestione dei rapporti con terzi, a riferirsi a principi equivalenti a quelli adottati da Digital Solutions in materia di corruzione e contemplino il diritto della Società alla risoluzione del contratto (con eventuale pagamento di penali).

- ***Con riferimento alla gestione di associazione temporanee di imprese o stipulazione e alla successiva gestione di contratti con Partner, la Società adotta procedure aziendali che prevedono:***

- i) l'esecuzione di preventivi controlli, verifiche ed accertamenti, il cui grado di accuratezza deve essere valutato in ragione della tipologia di attività, del Paese di riferimento e del grado di conoscenza già acquisito sulla controparte, volte ad accertare l'affidabilità, la professionalità e reputazione del *Partner*;
- ii) il coinvolgimento, laddove possibile, di più funzioni nel processo di negoziazione e gestione della *partnership*, con la definizione di ruoli e responsabilità;
- iii) l'inserimento di clausole contrattuali che impegnino i *Partner* al rispetto delle politiche anticorruptive, e del Modello adottati dalla Società e contemplino il diritto della Società alla risoluzione del contratto (con eventuale pagamento di penali) o altra idonea sanzione contrattuale in caso di violazione degli obblighi assunti.

In relazione alla selezione, amministrazione ed assunzione del personale la Società adotta procedure aziendali volte ad assicurare:

- i) che l'apertura del procedimento di assunzione sia effettuata esclusivamente sulla base di reali esigenze gestionali;
  - ii) che il processo di selezione veda il coinvolgimento di almeno due aree distinte e che lo stesso sia basato su criteri di oggettività, competenza e professionalità volti ad evitare favoritismi o clientelismi;
  - iii) che i sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna siano basati su *target* di *performance* sostanzialmente raggiungibili.
- ***Con riferimento alla gestione dei flussi finanziari e della tesoreria, la Società adotta procedure aziendali volte ad assicurare che:***
    - i) tutti i flussi finanziari in entrata e uscita siano adeguatamente identificabili e tracciabili, nonché correttamente e regolarmente registrati in appositi libri e registri contabili segregati ed il cui accesso è consentito solo ai soggetti espressamente autorizzati;
    - ii) tutti i flussi finanziari in entrata e in uscita siano supportati da specifica documentazione giustificativa, che riporti chiaramente e fedelmente le transazioni a cui fa riferimento;
    - iii) sia rispettato il principio di segregazione dei ruoli tra i soggetti che autorizzano, coloro che eseguono e coloro che controllano i flussi finanziari in entrata e uscita;
    - iv) il denaro contante sia utilizzato solo per le spese di piccola cassa e comunque per importi inferiori ad Euro 3.000,00 (tremila/00).
  - ***Con riferimento alla gestione dei rapporti con società di certificazione e con il revisore, la Società adotta procedure aziendali volte ad assicurare che:***
    - i) siano rispettate le fasi di valutazione e selezione della società di revisione contabile e della società di certificazione;

- ii) gli incarichi, diversi da quelle del bilancio d'esercizio e di revisione contabile, purché consentiti dalla legge e dai regolamenti, vengono conferiti alla società di revisione, previo parere del Collegio Sindacale;

Infine, per quanto non ivi previsto, si fa espresso rinvio al rispetto dei principi comportamentali e procedurali di cui alla Parte Speciale B relativa ai Reati Societari.

**PARTE SPECIALE D**

**DELITTI INFORMATICI, TRATTAMENTO  
ILLECITO DI DATI E REATI IN MATERIA DI  
VIOLAZIONE DEL DIRITTO D'AUTORE**

*Articoli 24-bis e 25-novies del Decreto Legislativo 231/2001*



# DIGITAL SOLUTIONS

## D.1. Funzione della Parte Speciale D.

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i Destinatari del Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dagli articoli 24-*bis* e 25-*novies* del Decreto e nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle proprie attività.

La presente Parte Speciale richiama ed integra quanto già disciplinato nel Documento Programmatico per la Sicurezza.

Nello specifico la presente Parte Speciale ha lo scopo di:

- a) indicare le procedure che i Destinatari sono chiamati ad osservare al fine di applicare correttamente le prescrizioni del Modello;
- b) fornire ai responsabili delle funzioni interne quali gli Organi Sociali o soggetti che cooperano con tali funzioni, nonché all'OdV, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

## D.2. Le fattispecie di Reato.

Di seguito si descrivono i Reati previsti nell'articolo 24-*bis* del Decreto Legislativo 231/2001 introdotti con l'articolo 7 della Legge di ratifica della Convenzione del Consiglio di Europa del 18 marzo 2008, n. 48, fatta a Budapest il 23 novembre 2001, sulla criminalità informatica e i reati previsti nell'articolo 25-*novies* del Decreto Legislativo 231/2001 in materia di violazione del diritto di autore.

### D.2.1. I reati informatici e trattamento illecito di dati (articolo 24-*bis* del Decreto).

#### **Falsità di un documento informatico pubblico o privato (articolo 491-*bis* del Codice Penale).**

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico. I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali. Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (articolo 1, comma 1, lettera p) Decreto Legislativo 82/2005, salvo modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato.

#### **Accesso abusivo ad un sistema informatico o telematico (articolo 615-*ter* del Codice Penale).**

La norma tutela la *privacy* informatica e telematica, ovvero la riservatezza dei dati memorizzati nei sistemi informatici o trasmessi con i sistemi telematici. Essa prevede due distinte condotte di reato:

## DIGITAL SOLUTIONS

quella dell'accesso abusivo in un sistema informatico o telematico protetto da misure di sicurezza, e quella di chi vi si mantiene contro la volontà espressa o tacita di chi ha diritto di escluderlo.

Sistema informatico è il complesso degli elementi fisici (*hardware*) e astratti (*software*) che compongono un apparato di elaborazione. Sistema telematico è qualsiasi sistema di comunicazione in cui lo scambio di dati e informazioni sia gestito con tecnologie informatiche e di telecomunicazione. La condotta di introduzione si realizza nel momento in cui l'agente oltrepassi abusivamente le barriere di protezione sia dell'*hardware* che del *software*. La legge non richiede che l'agente abbia preso conoscenza di tutti o di una parte cospicua dei dati memorizzati nel sistema violato. E' sufficiente, per la consumazione del reato, che abbia superato le barriere di protezione e che abbia iniziato a conoscere i dati in esso contenuti.

### **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (articolo 615-*quater* del Codice Penale).**

La condotta incriminata consiste alternativamente nel procurarsi, ovvero acquistare in qualsiasi modo la disponibilità (è del tutto irrilevante che il codice di accesso al sistema informatico altrui, oggetto di cessione, sia stato ottenuto illecitamente) riprodurre, ovvero effettuare la copia in uno o più esemplari, diffondere ovvero divulgare, comunicare, ovvero portare a conoscenza materialmente a terzi codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure nel fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza.

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'articolo 615-*quater* del Codice Penale, pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, *password* o schede informatiche (ad esempio, *badge*, carte di credito, *bancomat* e *smart card*).

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, *policy Internet*).

L'articolo 615-*quater*, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente della Società autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno della Società oppure carisca in altro modo fraudolento o ingannevole il codice di accesso.

### **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (articolo 615-*quinqies* del Codice Penale).**

La norma intende preservare il corretto funzionamento delle tecnologie informatiche. Essa sanziona la condotta di chiunque si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i

## DIGITAL SOLUTIONS

programmi in esso contenuti o a esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, l'alterazione del suo funzionamento.

Il riferimento è, tra l'altro, ai c.d. *virus*, programmi capaci di modificare o cancellare i dati di un sistema informatico.

### **Intercettazioni, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617-*quater* del Codice Penale).**

La norma in esame tutela la riservatezza delle comunicazioni informatiche ovvero il diritto all'esclusività della conoscenza del contenuto di queste ultime, sia nei confronti di condotte di indebita captazione, sia di rivelazione di contenuti illecitamente appresi. La condotta incriminata consiste alternativamente nell'intercettare, impedire o interrompere in modo fraudolento comunicazioni tra sistemi informatici.

### **Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (articolo 617-*quinqües* del Codice Penale).**

La norma tutela il bene giuridico della riservatezza delle informazioni o notizie trasmesse per via telematica o elaborate da singoli sistemi informatici. Il reato si perfeziona con la messa in opera delle apparecchiature idonee ad intercettare impedire o interrompere comunicazioni informatiche o telematiche.

### **Danneggiamento di informazioni, dati e programmi informatici (articolo 635-*bis* del Codice Penale).**

La norma punisce chiunque distrugge, deteriora, cancella, altera o sopprime informazioni dati e programmi informatici. La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia, ovvero con abuso della qualità di operatore di sistema.

### **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635-*ter* del Codice Penale).**

La norma sanziona la condotta di chiunque ponga in essere atti volti a distruggere, deteriorare, cancellare, alterare o a sopprimere informazioni dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità. La pena è aumentata qualora dal fatto consegua la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o programmi informatici.

### **Danneggiamento di sistemi informatici o telematici (articolo 635-*quater* del Codice Penale).**

La norma punisce le condotte di distruzione e danneggiamento di sistemi informatici o telematici altrui (o ostacolo al loro funzionamento) che si realizzano attraverso la distruzione e il danneggiamento delle informazioni, dei dati e dei programmi ovvero la loro introduzione o trasmissione.

### **Danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635-*quinqües* del Codice Penale).**

La norma sanziona la medesima condotta descritta al punto precedente, commessa in danno di sistemi informatici o telematici di pubblica utilità.

### **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (articolo 640-quinquies del Codice Penale).**

La norma sanziona la condotta di chi presta servizi di certificazione di firma elettronica, che, al fine di procurare a sé o ad altri un ingiusto profitto o di arrecare danno agli altri, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

### **D.2.2. I reati in materia di violazione del diritto d'autore (articolo 25-novies del Decreto).**

Si tratta di reati previsti dalla Legge 633/1941 a tutela del diritto d'autore. Segnatamente:

#### **Articolo 171, comma 1, lettera a-bis) e comma 3 della Legge 22 aprile 1941, n. 633.**

Tale norma reprime la condotta di chi, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, 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.

È previsto un aggravio di pena se la condotta è commessa sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Ai sensi del secondo comma, è possibile estinguere il reato pagando, prima dell'apertura del dibattimento o prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena pecuniaria stabilita dal comma primo, oltre alle spese del procedimento.

Tale articolo incrimina il c.d. "peer-to-peer"<sup>5</sup>, indicando però solamente l'immissione in *internet* di opere dell'ingegno protette, e non anche le condotte successive di condivisione e diffusione mediante le quali chiunque può accedere alle opere inserite nella rete telematica.

L'oggetto della tutela è rappresentato dalle opere dell'ingegno protette, da intendersi, secondo le definizioni:

- i) dell'articolo 1 della Legge 633/1941, secondo cui *"Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione. Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore"*<sup>6</sup>;

---

<sup>5</sup>Il *peer-to-peer* è lo scambio di opere protette che avviene nei sistemi di *file-sharing*, nei quali ciascun utente è sia *downloader* che *uploader* poiché automaticamente condivide i file scaricati anche durante la fase di *download*.

<sup>6</sup>L'articolo 2 specifica quali opere sono oggetto della tutela, disponendo che *"In particolare sono comprese nella protezione: 1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto se in forma scritta quanto se orale; 2) le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originale; 3) le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti; 4) le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia; 5) i disegni e le opere dell'architettura; 6) le opere dell'arte cinematografica, muta o sonora, sempreché non si tratti di semplice documentazione protetta ai sensi delle norme del capo quinto del titolo secondo; 7) le opere fotografiche e quelle espresse con procedimento analogo a quello della fotografia sempre che non si tratti di semplice fotografia protetta ai sensi delle norme del capo V del titolo II; 8) i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso; 9) le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto; 10) le opere del disegno industriale che presentino di per sé carattere creativo e valore artistico"*.

- ii) dell'articolo 2575 del Codice Civile, per il quale *“Formano oggetto del diritto di autore<sup>7</sup> le opere dell'ingegno di carattere creativo che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia qualunque ne sia il modo o la forma di espressione”*.

### **Articolo 171-bis della Legge del 22 aprile 1941, n. 633.**

La norma in esame prevede due ipotesi di reato:

- i) al primo comma, viene punita la condotta di chi 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 altresì perseguito penalmente il medesimo comportamento se inerente a 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;
- ii) al secondo comma, viene punita la condotta di chi, 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 o esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di legge, ovvero distribuisce, vende o concede in locazione una banca di dati.

### **Articolo 171-ter della Legge 22 aprile 1941, n. 633.**

Il comma primo della norma in esame punisce una serie di condotte se realizzate per un uso non personale e a fini di lucro; nello specifico sono sanzionate:

- i) l'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero di ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
- ii) l'abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento, di opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
- iii) fuori dai casi di concorso nella duplicazione o riproduzione, l'introduzione nel territorio dello Stato, la detenzione per la vendita o la distribuzione, la distribuzione, la messa in commercio, la concessione in noleggio o la cessione a qualsiasi titolo, la proiezione in pubblico, la trasmissione a mezzo della televisione con qualsiasi procedimento, la trasmissione a mezzo della radio, il far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui sopra;
- iv) la detenzione per la vendita o la distribuzione, la messa in commercio, la vendita, il noleggio, la cessione a qualsiasi titolo, la proiezione in pubblico, la trasmissione a mezzo della radio o della televisione con qualsiasi procedimento, di videocassette, musicassette, qualsiasi

---

<sup>7</sup> Il contenuto del diritto d'autore è definito dall'articolo 2577 c.c., che dispone che *“L'autore ha il diritto esclusivo di pubblicare l'opera e di utilizzarla economicamente in ogni forma e modo, nei limiti e per gli effetti fissati dalla legge. L'autore, anche dopo la cessione dei diritti previsti dal comma precedente, può rivendicare la paternità dell'opera e può opporsi a qualsiasi deformazione, mutilazione o altra modificazione dell'opera stessa, che possa essere di pregiudizio al suo onore o alla sua reputazione”* e dall'articolo 12 della l. 633/1941, il quale prevede che l'autore abbia il diritto esclusivo di pubblicare l'opera e di utilizzare economicamente l'opera nei limiti fissati dalla legge.

## DIGITAL SOLUTIONS

supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o altro supporto per il quale è prescritta, ai sensi della legge sul diritto d'autore, l'apposizione di contrassegno da parte della SIAE, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

- v) la ritrasmissione o diffusione con qualsiasi mezzo di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato, in assenza di accordo con il legittimo distributore;
- vi) l'introduzione nel territorio dello Stato, la detenzione per la vendita o la distribuzione, la distribuzione, la vendita, la concessione in noleggio, la cessione a qualsiasi titolo, la promozione commerciale, l'installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;
- vii) la fabbricazione, l'importazione, la distribuzione, la vendita, il noleggio, la cessione a qualsiasi titolo, la pubblicizzazione per la vendita o il noleggio, la detenzione per scopi commerciali di attrezzature, prodotti o componenti ovvero la prestazione di servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di prevenzione ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure;
- viii) l'abusiva rimozione o alterazione delle informazioni elettroniche che identificano l'opera o il materiale protetto, nonché l'autore o qualsiasi altro titolare dei diritti ai sensi della legge sul diritto d'autore, ovvero la distribuzione, l'importazione a fini di distribuzione, la diffusione per radio o per televisione, la comunicazione o la messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le suddette informazioni elettroniche.

Il secondo comma della norma in esame invece punisce:

- i) l'abusiva riproduzione, duplicazione, trasmissione, diffusione, vendita, messa in commercio, cessione a qualsiasi titolo o importazione di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
- ii) la comunicazione al pubblico a fini di lucro e in violazione delle disposizioni sul diritto di comunicazione al pubblico dell'opera, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa<sup>8</sup>;
- iii) la realizzazione di un comportamento previsto dal primo comma da parte di chi esercita in forma imprenditoriale attività di riproduzione, distribuzione, vendita, commercializzazione o importazione di opere tutelate dal diritto d'autore e da diritti connessi;
- iv) la promozione o l'organizzazione delle attività illecite di cui al comma primo.

Il terzo comma prevede un'attenuante se il fatto è di particolare tenuità, mentre il comma quarto prevede alcune pene accessorie, ovvero la pubblicazione della sentenza di condanna, l'interdizione da una professione o da un'arte, l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese e la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

---

<sup>8</sup> Tale condotta risulta assai simile a quella prevista dall'articolo 171, comma 1, lett. *a-bis*), ma si distingue da quest'ultima in quanto prevede il dolo specifico del fine di lucro e la comunicazione al pubblico in luogo della messa a disposizione dello stesso.

### **Articolo 171-septies della Legge 22 aprile 1941, n. 633.**

La norma in analisi prevede l'applicazione della pena comminata per le condotte di cui al primo comma dell'articolo 171-ter anche per:

- i) i produttori o importatori dei supporti non soggetti al contrassegno SIAE, i quali non comunicano alla medesima entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;
- ii) chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi.

### **Articolo 171-octies della Legge 22 aprile 1941, n. 633.**

La norma in esame reprime la condotta di chi, a fini fraudolenti, produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

Sebbene tale fattispecie presenti profili di sovrapposizione con quella prevista dalla lettera f) del secondo comma dell'articolo 171-ter, le stesse si differenziano per una serie di ragioni:

- la pena comminata dall'articolo 171-octies è più grave di quella comminata dall'articolo 171-ter (uguale la reclusione, ma maggiore la multa): quindi non scatta la applicazione della clausola che esclude il primo reato se il fatto costituisca anche un reato più grave;
- le condotte incriminate non sono perfettamente sovrapponibili;
- il dolo è differente, richiedendosi il fine di lucro per il reato di cui all'articolo 171-ter e il fine fraudolento per il reato di cui all'articolo 171-octies;
- diverso è almeno in parte il tipo di trasmissione protetta, giacché l'articolo 171-ter fa riferimento a trasmissioni rivolte a chi paga un canone di accesso, mentre l'articolo 171-octies si riferisce a trasmissioni rivolte a utenti selezionati indipendentemente dal pagamento di un canone.

### **D.3. Aree di Rischio ed Attività Sensibili.**

Le Aree a Rischio della Società, con riferimento ai delitti informatici e trattamento illecito di dati ed ai reati in materia di violazione del diritto d'autore sono riconducibili principalmente alla gestione della sicurezza informatica.

I delitti di cui ai capitoli che precedono trovano come presupposto l'utilizzo della rete informatica intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi anche se, nel caso di specie, il servizio di gestione del sistema informatico ("IT") di Digital Solutions.



## DIGITAL SOLUTIONS

In particolare sono state identificate le seguenti Attività Sensibili:

Con specifico riferimento ai delitti informatici e trattamento illecito dei dati:

- *la gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica ed applicativa, nonché la gestione della sicurezza informatica;*
- *l'utilizzo ed accesso alla rete aziendale, al servizio di posta elettronica e l'accesso ad internet sia per le utenze interne sia per le esterne.*

Con specifico riferimento ai delitti in materia di diritto d'autore:

- *utilizzo degli applicativi informatici aziendali, in considerazione del potenziale utilizzo senza licenza di software coperti da altrui diritto d'autore;*
- *gestione di contenuti multimediali sulla rete aziendale ed in particolare sul sito internet;*
- *riproduzione, duplicazione e divulgazione di opere di ingegno coperte dal diritto d'autore.*

### **D.4. Principi generali di comportamento.**

Obiettivo della presente Parte Speciale è che i Destinatari, inclusi i Terzi ovvero i soggetti che operano a livello periferico (Consulenti, *service provider* etc.) nella misura in cui gli stessi possano essere coinvolti nelle Aree di Rischio e nelle Attività Sensibili, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei delitti informatici.

Nell'espletamento delle attività aziendali e, in particolare, delle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto instaurato con la Società, di porre in essere comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle qui considerate.

In particolare non è ammesso:

- i) porre in essere quei comportamenti che integrano le fattispecie di reato o che, sebbene non costituiscano di per sé un'ipotesi di reato, possano esserne il presupposto (ad esempio, mancato controllo);
- ii) divulgare informazioni relative ai sistemi informatici aziendali;
- iii) utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta o comunque contrarie a quanto previsto nel Modello e nel Codice Etico;
- iv) utilizzare illecitamente materiale tutelato da altrui diritto d'autore.

Nell'espletamento delle rispettive attività/funzioni oltre alle regole di cui al Modello e nel presente capitolo, i Destinatari, come sopra meglio individuati, sono tenuti a conoscere ed osservare tutte le regole e i principi contenuti nei seguenti documenti:

- i) le procedure aziendali relative alla gestione degli accessi logici a reti, sistemi, dati e applicazioni e della piattaforma informatica;
- ii) la procedura aziendale relativa alla gestione delle credenziali personali (*username* e *password*);



## DIGITAL SOLUTIONS

- iii) l'impegno alla corretta gestione delle informazioni di cui si viene a conoscenza per ragioni operative.

Al fine di mitigare il rischio di commissione dei delitti informatici e, di conseguenza, anche di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti lo svolgimento della propria attività, si è dotata di Certificazione ISO 9001 e Certificazione ISO 27001 assolvendo ai seguenti adempimenti:

- i) fornire, ai Destinatari, un'adeguata informazione circa il corretto utilizzo degli *user-id* e delle *password* per accedere ai principali sottosistemi informatici utilizzati presso la Società;
- ii) limitare, attraverso abilitazioni di accesso differenti, l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi;
- iii) predisporre e mantenere adeguate difese fisiche a protezione dei *server* della Società;
- iv) predisporre e mantenere adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

### D.5. Principi specifici di comportamento.

#### *Gestione della sicurezza informatica.*

Al fine dell'attuazione delle regole e del rispetto dei divieti elencati al precedente capitolo, devono essere ottemperati i principi procedurali qui di seguito descritti, oltre alle regole ed ai principi già contenuti nella Parte Generale del Modello.

La Società svolge attività di strutturazione, monitoraggio, difesa del patrimonio informatico e telematico aziendale.

In particolare la Società:

- i) stabilisce i requisiti dei sistemi IT;
- ii) ha identificato i soggetti che utilizzano ed hanno accesso agli stessi mediante censimento;
- iii) qualifica le risorse economiche e finanziarie da assegnare alla gestione e sviluppo della struttura stessa;
- iv) adotta sistemi di protezione da eventuali accessi esterni e da eventuali manomissioni da parte degli utenti interni;
- v) stabilisce e divulga le regole di utilizzo degli strumenti informatici e dei *software* della Società.

Si elencano qui di seguito le regole che devono essere rispettate dai Destinatari della presente Parte Speciale nell'Ambito delle Attività Sensibili identificate.

- ***Gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica ed applicativa, nonché gestione della sicurezza informatica.***
  - i) i *server* applicativi centralizzati devono essere ospitati in locali dedicati e messi in sicurezza;

## DIGITAL SOLUTIONS

- ii) l'accesso ai suddetti locali deve essere riservato al solo personale IT;
- iii) la rete deve essere protetta da *firewalls* e da *software antivirus/antispam*, ripetutamente aggiornati nel corso della giornata;
- iv) i *backup* dei dati residenti sui *server* devono essere salvati con frequenza giornaliera ed i supporti adeguatamente conservati.
- ***Utilizzo ed accesso alla rete aziendale, al servizio di posta elettronica e l'accesso ad internet sia per le utenze interne sia per le esterne.***
  - i) tutte le nuove utenze devono essere attivate previo invio di una richiesta predisposta da un responsabile di funzione;
  - ii) i profili di accesso sono nominativi e richiedono l'inserimento di *password* personali, che devono essere modificate periodicamente;
  - iii) sono assegnati diversi poteri e restrizioni, a seconda della tipologia di profilo (utente o amministratore);
  - iv) l'accesso logico ai sistemi informativi deve essere protetto da *user id e password* utente con scadenza massima di 180 giorni;
  - v) le credenziali di accesso ai sistemi devono essere prontamente eliminate per il personale dimesso e ogni utente deve disporre di *user id e password* personale.
- ***Utilizzo degli applicativi informatici aziendali e gestione di contenuti multimediali.***
  - i) le installazioni di nuovi *software* devono essere effettuate previa verifica del possesso delle relative licenze;

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione dei sistemi informativi aziendali è fatto obbligo di:

- i) utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- ii) custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- iii) aggiornare periodicamente le *password*;
- iv) garantire la tracciabilità dei documenti prodotti attraverso l'archiviazione delle varie versioni dei documenti o comunque garantire meccanismi di tracciabilità delle modifiche;
- v) assicurare meccanismi di protezione dei file, quali *password*, conversione dei documenti in formato non modificabile.
- ***Riproduzione, duplicazione e divulgazione di opere di ingegno coperte dal diritto d'autore.***

A tutti i Dipendenti è inoltre vietato di:

- i) utilizzare immagini, video, composizioni musicali, banche dati ovvero qualsiasi opera dell'ingegno protetta dal diritto d'autore senza aver ottenuto le necessarie licenze e permessi;

## DIGITAL SOLUTIONS

- ii) utilizzare immagini, video o composizioni musicali senza aver sottoscritto specifici accordi a tutela della Società;
- iii) riprodurre opere dell'ingegno (quali ad esempio libri o manuali) se non nei limiti previsti dalla legge tempo per tempo vigente e per sola finalità di agevolare la lettura e l'esame delle tematiche ivi trattate.

La Società fornisce alle funzioni interessate adeguata informazione e formazione circa le potenziali rischiosità in materia di responsabilità amministrativa degli enti connesse all'attività di gestione e pubblicazione di contenuti in *streaming*, sul sito *internet* della Società.

**PARTE SPECIALE E**

**DELITTI DI CRIMINALITÀ ORGANIZZATA, DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI E UTILITÀ DI PROVENIENZA ILLECITA NONCHÉ DI AUTORICICLAGGIO**

**E**

**DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO**

**Articoli *24-ter*, *25-octies*, *25-quater* e del Decreto Legislativo 231/2001**

## DIGITAL SOLUTIONS

### E.1 Funzione della Parte Speciale E.

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i Destinatari del Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato richiamate dagli articoli 24-ter, 25-octies e 25-quater del Decreto Legislativo 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di:

- a) definire le procedure che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- b) supportare l'Organismo di Vigilanza e i responsabili delle altre funzioni aziendali ad esercitare le attività di controllo, monitoraggio e verifica.

### E.2 Fattispecie di Reato rilevanti.

Per completezza, di seguito vengono riportate tutte le fattispecie di reato che fondano la responsabilità amministrativa degli enti ai sensi degli articoli 24-ter, 25-octies e 25-quater del Decreto.

#### E.2.1 Delitti di criminalità organizzata (articolo 24-ter del Decreto).

##### **Associazione per delinquere (articolo 416 del Codice Penale).**

Il reato punisce chi promuove, costituisce o organizza associazioni di tre o più persone con il fine di commettere più delitti.

##### **Associazione di tipo mafioso anche straniera (articolo 416-bis del Codice Penale).**

Il reato punisce chi fa parte di un'associazione di tipo mafioso formata da tre o più persone, anche straniera.

##### **Scambio elettorale politico-mafioso (articolo 416-ter del Codice Penale).**

Il reato punisce chi ottiene la promessa di voti in cambio di erogazione di denaro.

##### **Sequestro di persona a scopo di estorsione (articolo 630 del Codice Penale).**

Il reato si realizza allorché taluno sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione.

##### **Associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (articolo 74 D.P.R.309/1990).**

Il reato punisce chi promuove, costituisce, dirige, organizza o finanzia associazioni di tre o più persone con il fine di commettere più delitti tra quelli previsti dall'articolo 73 del D.P.R. 309/1990.

**Delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (articolo 407, comma 2, lettera a), numero 5 del Codice di Procedura Penale).**

## DIGITAL SOLUTIONS

### E.2.2 Delitti con finalità di terrorismo ed eversione dell'ordine democratico (articolo 25-*quater* del Decreto).

L'articolo 25-*quater* del Decreto non fornisce un'esatta indicazione "numerica" dei titoli di reato riconducibili entro i confini della sanzionabilità a carico dell'ente, ma si riferisce, genericamente, "alla commissione di dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previste dal codice penale e dalle leggi speciali".

Si possono ritenere reati rilevanti, ai sensi dell'articolo 25-*quater*, le seguenti fattispecie criminose:

- i) associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (articolo 270-*bis* del Codice Penale);
- ii) assistenza agli associati (articolo 270-*ter* del Codice Penale);
- iii) arruolamento con finalità di terrorismo anche internazionale (articolo 270-*quater* del Codice Penale);
- iv) organizzazione di trasferimenti per finalità di terrorismo (articolo 270-*quater*.1 del Codice Penale);
- v) addestramento ad attività con finalità di terrorismo anche internazionale (articolo 270-*quinquies* del Codice Penale);
- vi) condotte con finalità di terrorismo (articolo 270-*sexies* del Codice Penale);
- vii) attentato per finalità terroristiche o di eversione (articolo 280 del Codice Penale);
- viii) atto di terrorismo con ordigni micidiali o esplosivi (articolo 280-*bis* del Codice Penale);
- ix) sequestro di persona a scopo di terrorismo o di eversione (articolo 630 del Codice Penale).

### E.2.3 Delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché auto-riciclaggio (articolo 25-*octies* del Decreto).

#### **Ricettazione (articolo 648 del Codice Penale).**

Il reato di ricettazione punisce chi acquista, riceve, occulta o si intromette nell'acquistare, ricevere o occultare denaro o cose provenienti da un qualsiasi delitto. Tale condotta è finalizzata alla realizzazione di un profitto a favore dell'autore stesso o di un terzo. Perché sussista ricettazione è necessario che l'autore del reato non abbia concorso alla realizzazione del delitto dal quale provengono il denaro o le cose oggetto di ricettazione.

#### **Riciclaggio (articolo 648-*bis* del Codice Penale).**

La fattispecie di riciclaggio si configura ogni qualvolta taluno, sostituisce o trasferisce denaro, beni o altre utilità provenienti da un delitto non colposo ovvero compie in relazione ad essi altre operazioni. La condotta perché sia rilevante deve essere tale da ostacolare l'identificazione della provenienza delittuosa del denaro, dei beni o delle altre utilità. Così come per la ricettazione, anche il riciclaggio sussiste fuori dai casi di concorso dal delitto dal quale provengono il denaro, i beni o le altre utilità.

Nella condotta di "sostituzione" rientra ogni attività diretta a incidere sul compendio criminoso separando ogni possibile collegamento con il reato. Le concrete modalità operative possono consistere in operazioni bancarie, finanziarie, commerciali, attraverso le quali si scambiano le utilità economiche

## DIGITAL SOLUTIONS

di provenienza illecita con altre lecite; ovvero con il cambio di cartamoneta in valute diverse, con speculazioni sui cambi, con l'investimento del danaro in titoli di Stato, azioni etc.

### **Impiego di denaro beni o utilità di provenienza illecita (articolo 648-ter del Codice Penale).**

Il reato di impiego di denaro punisce chiunque, fuori dai casi di concorso nel reato e fuori dai casi di ricettazione e riciclaggio sopra richiamati, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

La condotta punibile è descritta con il verbo impiegare, che non ha una precisa valenza tecnica e finisce con l'aver una portata particolarmente ampia, potendosi attingere a qualunque forma di utilizzazione di utilizzazione di denaro, beni o altre utilità provenienti da delitto indipendentemente da qualsiasi obiettivo o risultato utile per l'agente.

### **Auto-riciclaggio (articolo 648-ter.1 del Codice Penale).**

Il reato punisce chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

### **E.3 Aree di rischio ed Attività Sensibili.**

Le Aree di Rischio della Società, con riferimento ai delitti di criminalità organizzata, ricettazione, riciclaggio, impiego di denaro, beni e utilità di provenienza illecita nonché auto-riciclaggio e delitti con finalità di terrorismo ed eversione dell'ordine democratico, sono riconducibili a:

- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*
- *Gestione dei flussi finanziari e predisposizione delle scritture contabili;*
- *Selezione e gestione di segnalatori, sviluppatori e partner commerciali;*
- *Gestione e selezione delle assunzioni del personale e del sistema premiante;*
- *Gestione dei rapporti con società di certificazione e con il revisore.*

### **E.4 Principi generali di comportamento.**

Obiettivo del presente capitolo è che i Destinatari si attengano, nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento delle Attività Sensibili, individuate nella presente Parte Speciale, a regole di condotta conformi a quanto qui prescritto, oltre al rispetto del Codice Etico e delle *policy* aziendali.

In particolare, la Società adotta i seguenti principi generali, a cui i Destinatari devono attenersi:

- a) la segregazione dei ruoli;
- b) la valutazione comparativa di più offerte contrattuali, salvo deroghe disciplinate da apposite procedure aziendali;
- c) la formalizzazione e tracciabilità degli acquisti dall'attivazione alla fine;
- d) la verifica della congruità dei corrispettivi negoziati ed attività svolte;

## DIGITAL SOLUTIONS

- e) la forma scritta dell'accordo e l'indicazione nello stesso del compenso pattuito o delle modalità con cui determinare lo stesso;
- f) l'adozione di modalità di pagamento che escludano l'utilizzo di conti non intestati al consulente/fornitore e, in ogni caso, escludano pagamenti in contanti;
- g) la predisposizione di albo fornitori ovvero di apposite liste di consulenti e di fornitori già preventivamente qualificati e la cui presenza nell'albo viene periodicamente rivalutata;
- h) l'inserimento nei contratti di clausole che impegnino i consulenti e i fornitori, nella conduzione dei propri affari e nella gestione dei rapporti con terzi, a riferirsi a principi equivalenti a quelli adottati da Digital Solutions in materia di corruzione e contemplino il diritto della Società alla risoluzione del contratto (con eventuale pagamento di penali).

Inoltre la Società deve provvedere a:

- a) instaurare rapporti esclusivamente con controparti che godano di una comprovata reputazione e rispettabilità e la cui cultura etica aziendale sia comparabile a quella della Società;
- b) assicurare la trasparenza degli accordi ed evitare la sottoscrizione di patti o accordi contrari alla legge;
- c) mantenere con le controparti rapporti trasparenti e collaborativi;
- d) segnalare tempestivamente all'OdV ogni comportamento della controparte che appaia contrario ai principi etici di cui al Codice Etico;
- e) gestione trasparente degli acquisti di beni e servizi, dei flussi finanziarie dei rapporti *inter-company*.

### E.5 Principi specifici di comportamento.

Per i principi specifici di comportamento relativi alle seguenti Attività Sensibili, ovvero:

- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*
- *Gestione dei flussi finanziari e predisposizione delle scritture contabili;*
- *Gestione delle assunzioni del personale e del sistema premiante;*
- *Selezione e gestione di segnalatori, sviluppatori e partner commerciali*

si rinvia a quanto previsto nella Parte Speciale A “*Reati commessi nei rapporti con la Pubblica Amministrazione e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria*” nella Parte Speciale B “*Reati Societari*” e nella Parte Speciale C “*Reati di corruzione tra privati*”



**PARTE SPECIALE F**

**DELITTI DI OMICIDIO COLPOSO E LESIONI PERSONALI COLPOSE GRAVI E GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME A TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO**

**E**

**DELITTO DI IMPIEGO DI CITTADINI DI STATI TERZI IL CUI SOGGIORNO È IRREGOLARE**

**Articoli *25-septies* e *25-duodecies* del Decreto Legislativo 231/2001**

### Definizioni.

Si rinvia alle definizioni di cui alla Parte Generale, fatte salve le ulteriori definizioni contenute nella presente Parte Speciale.

“ASPP” o “Addetti al Servizio di Prevenzione e Protezione”: i soggetti in possesso della capacità e dei requisiti professionali di cui all’articolo 32 del Testo Unico Sicurezza designati per l’espletamento dei compiti rientranti nel Servizio di Prevenzione e Protezione.

“BS – OHSAS 18001 o British Standard”: *British Standard OHSAS 18001:2007*, a cui la Società si è ispirata per la predisposizione della presente Parte Speciale.

“Datore di Lavoro”: il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l’assetto dell’organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità, in virtù di apposita delega, dell’organizzazione stessa o del singolo settore in quanto esercita i poteri decisionali e di spesa.

“Testo Unico Sicurezza” o “D.Lgs. 81/2008”: il Decreto Legislativo del 9 aprile 2008, n. 81 “*Attuazione dell’articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro*”.

“Delegato Sicurezza”: il dirigente ex articolo 18 D.Lgs. 81/2008 ai quali il Datore di Lavoro può delegare, ai sensi dell’articolo 16 del D.Lgs. 81/2008, funzioni di responsabilità relative alla salute e sicurezza sul lavoro eventualmente nominati all’interno della Società.

“DUVRI” o “Documento Unico di Valutazione dei Rischi per le Interferenze”: il documento redatto dal Datore di Lavoro committente contenente una valutazione dei rischi e che indichi le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze.

“DVR” o “Documento di Valutazione dei Rischi”: il documento redatto dal Datore di Lavoro contenente una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l’attività lavorativa ed i criteri per la suddetta valutazione, l’indicazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuali adottati a seguito di tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l’individuazione delle procedure per l’attuazione delle misure da realizzare nonché dei ruoli dell’organizzazione aziendale che vi debbono provvedere, l’indicazione dei nominativi di RSPP, RLS e del Medico Competente che ha partecipato alla valutazione del rischio, nonché l’individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione ed addestramento.

“Impresa affidataria”: impresa titolare del contratto di appalto con il committente che, nell’esecuzione dell’opera appaltata, può avvalersi di imprese subappaltatrici o di lavoratori autonomi;

“Impresa esecutrice”: impresa che esegue un’opera o parte di essa impegnando proprie risorse umane e/o propri materiali.

## DIGITAL SOLUTIONS

“Lavoratore”: persona che, indipendentemente dalla tipologia contrattuale, svolge un’attività lavorativa nell’ambito dell’organizzazione della Società con o senza retribuzione anche al fine di intraprendere un mestiere.

“Linee guida Uni-Inail”: le linee guida elaborate dall’UNI e dall’INAIL per la costituzione volontaria da parte delle imprese di un sistema di gestione della salute e sicurezza sul lavoro del 28 settembre 2001.

“Medico Competente”: il medico in possesso di uno dei titoli e dei requisiti formali e professionali indicati nel Testo Unico Sicurezza che collabora con il Datore di Lavoro della Società ai fini della valutazione dei rischi e al fine di effettuare la Sorveglianza Sanitaria ed adempiere tutti gli altri compiti di cui al Testo Unico Sicurezza.

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

“RSPP” o “Responsabile del Servizio di Prevenzione e Protezione”: il soggetto in possesso delle capacità e dei requisiti professionali indicati nel Testo Unico Sicurezza, designato dal Datore di Lavoro, a cui risponde, per coordinare il Servizio di Prevenzione e Protezione dai rischi.

“Sorveglianza Sanitaria”: l’insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei Lavoratori in relazione all’ambiente di lavoro, ai fattori di rischio professionale, ed alle modalità di svolgimento dell’attività lavorativa.

“SPP” o “Servizio di Prevenzione e Protezione”: l’insieme delle persone, sistemi e mezzi esterni o interni alla Società finalizzati all’attività di prevenzione e protezione dai rischi professionali per i Lavoratori.

“SSL”: Salute e Sicurezza dei Lavoratori.

### F.1. Funzione della Parte Speciale F.

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i Destinatari del presente Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dall'articoli 25-*septies* e 25-*duodecies* del Decreto Legislativo 231/2001.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- a) definire le procedure che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- b) supportare l'Organismo di Vigilanza e i responsabili delle altre funzioni aziendali ad esercitare le attività di controllo, monitoraggio e verifica.

### F.2. Fattispecie di Reato rilevanti.

#### F.2.1. I delitti di omicidio colposo e lesioni personali colpose gravi e gravissime commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro.

L'articolo 25-*septies* del Decreto prevede l'applicazione di sanzioni pecuniarie ed interdittive agli enti i cui esponenti commettano i reati di cui agli articoli 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del Codice Penale, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Le fattispecie delittuose riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica" che richiede che l'evento si verifichi a causa della inosservanza delle norme sulla salute e sicurezza sul lavoro.

**Omicidio colposo** (articolo 589 del Codice Penale): vi incorre chiunque cagioni per colpa la morte di una persona.

**Lesioni personali colpose** (articolo 590, 3 comma del Codice Penale): vi incorre chiunque cagioni ad altri per colpa una lesione personale grave o gravissima.

La lesione personale è **grave** (articolo 583, 1 comma del Codice Penale):

- i) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
- ii) se il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione personale è **gravissima** (articolo 583, 2 comma del Codice Penale) se dal fatto deriva:

- i) una malattia certamente o probabilmente insanabile;
- ii) la perdita di un senso;
- iii) 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;

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

Ai sensi dell'articolo 30 del Testo Unico Sicurezza *“in sede di prima applicazione i modelli di organizzazione aziendale definiti conformemente alle Linee Guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro del 28 settembre 2001, o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti”*.

Nella predisposizione di tale Parte Speciale si è tenuto conto dei principi cardine dei sistemi di gestione indicati dalle suddette linee guida, al fine di garantire il rispetto, da parte dei Destinatari, di regole minime di comportamento in relazione alla determinazione della politica aziendale in tema di sicurezza, alla relativa pianificazione degli obiettivi, alla messa in atto di opportune azioni di monitoraggio, alla sensibilizzazione del personale ed, infine, al periodico riesame del sistema in essere, al fine di valutarne la sua efficacia ed efficienza.

### **F.2.2. Impiego di cittadini di Stati terzi il cui soggiorno è irregolare (articolo 22, comma 12 e 12-bis del Decreto Legislativo 286/1998).**

Tale ipotesi di reato si configura nei confronti del datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo o sia stato revocato o annullato.

L'articolo 22, comma 12-bis del Decreto Legislativo 286/1998 prevede un aumento delle pene da un terzo alla metà qualora ricorrano le seguenti ipotesi:

- i) se i lavoratori occupati sono in numero superiore a tre;
- ii) se i lavoratori occupati sono minori in età non lavorativa;
- iii) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale (vale a dire, oltre alle ipotesi sopra citate, se i lavoratori sono esposti a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro).

La responsabilità dell'Ente è configurabile soltanto quando il reato in questione sia aggravato dal numero dei soggetti occupati o dalla minore età degli stessi o, infine, dalla prestazione del lavoro in condizioni di pericolo grave.

Per il Reato di impiego di cittadini di Paesi terzi con soggiorno irregolare all'Ente può essere applicata una sanzione pecuniaria da 100 a 200 quote, entro il limite di Euro 150.000,00 (centocinquantamila/00).

### **F.3. Aree di Rischio ed Attività Sensibili.**

#### **F.3.1. Attività Sensibili nell'ambito della Sicurezza nei luoghi di lavoro.**

Partendo dall'assunto che tutte le aree e tutti gli ambienti nei quali si svolge l'attività lavorativa dell'impresa in rapporto di dipendenza o di collaborazione, nonché le attività lavorative esterne svolte per conto dell'impresa, sono esposte al rischio infortunistico, notevole importanza assumono le attività di verifica degli adempimenti richiesti dalle normative antinfortunistiche e di tutela dell'igiene e della salute sul lavoro, nonché le procedure informative sulla gestione delle strutture (locali, arredi, macchinari, etc.) e sulla valutazione sanitaria degli ambienti di lavoro.

## DIGITAL SOLUTIONS

Di seguito sono elencate, al fine puramente esemplificativo, alcune delle Attività Sensibili svolte dal personale presso la sede della Società o in trasferta, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati qui considerati:

- *attività connesse ai tipici rischi d'ufficio (ad es. postura, videoterminale, rischio elettrico);*
- *attività svolte da personale esterno presso Terzi, quali ad esempio i fornitori di servizi in base a contratti di appalto, d'opera o di somministrazione (articolo 26 del Testo Unico Sicurezza);*
- *trasferte del personale.*

Specifica attenzione viene poi rivolta alle attività affidate a ditte appaltatrici e che operano per conto e/o in favore della Società.

### F.3.2. Attività Sensibili nell'ambito del delitto di impiego di cittadini di Stati terzi il cui soggiorno è irregolare.

Di seguito sono elencate le Attività Sensibili che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati qui considerati:

- *selezione del personale;*
- *attività svolte da personale esterno presso le sedi della Società, quali ad esempio i fornitori di servizi in base a contratti di appalto, d'opera o di somministrazione.*

### F.4 Il sistema di prevenzione in generale.

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei Lavoratori così come individuati dall'articolo 15 del Testo Unico Sicurezza ed in ottemperanza a quanto previsto dagli articoli 18, 19 e 20 del medesimo Decreto Legislativo 81/2008, nonché della normativa in materia di contrasto al lavoro irregolare, si prevede quanto segue.

#### a. La politica aziendale in tema di salute e sicurezza e la politica aziendale relativa al tema di assunzione del personale.

La Società ha adottato una politica per la sicurezza e salute sul lavoro che deve essere un riferimento fondamentale per tutti i Dipendenti, ponendosi come obiettivo quello di enunciare i principi cui deve ispirarsi ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte, nell'ottica della salute e sicurezza di tutti i Lavoratori.

Tale politica contiene:

- i) una chiara affermazione della responsabilità dell'intera organizzazione aziendale, dal Datore di Lavoro ai singoli Lavoratori, nella gestione delle tematiche relative alla salute e sicurezza sul lavoro, ciascuno per le proprie attribuzioni e competenze;
- ii) l'impegno a considerare tali tematiche come parte integrante della gestione aziendale;
- iii) l'impegno al miglioramento continuo ed alla prevenzione;
- iv) l'impegno a fornire le risorse umane e strumentali necessarie;
- v) l'impegno all'utilizzo esclusivo di personale regolare (sia esso personale dipendente o di terzi), anche tramite l'adozione di procedure che garantiscano il controllo e il monitoraggio

della validità dei permessi di soggiorno dei lavoratori provenienti da Paesi terzi. Nello specifico è fatto assoluto divieto di assumere o comunque impiegare lavoratori stranieri privi di regolare permesso di soggiorno;

- vi) l'impegno a garantire che i Destinatari, nei limiti delle rispettive attribuzioni, siano sensibilizzati a svolgere la propria attività nel rispetto degli obblighi di legge a tutela della salute e della sicurezza, del lavoro minorile e delle donne nonché delle condizioni igienicosanitarie dei lavoratori;
- vii) l'impegno al coinvolgimento ed alla consultazione dei Lavoratori, anche attraverso RLS;
- viii) l'impegno ad un riesame periodico della politica per la salute e sicurezza adottato al fine di garantire la sua costante adeguatezza alla struttura organizzativa della Società.

### **b. Il processo di pianificazione.**

La Società, con cadenza periodica:

- i) definisce gli obiettivi finalizzati al mantenimento e/o miglioramento delle misure di prevenzione e protezione;
- ii) predispose un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità;
- iii) definisce le risorse, anche economiche, necessarie;
- iv) prevede le modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi.

### **c. L'organizzazione del sistema.**

#### **Compiti e responsabilità.**

Nella definizione dei compiti organizzativi ed operativi dei Lavoratori, devono essere esplicitati e resi noti anche gli aspetti relativi alla sicurezza sul lavoro di loro competenza, gli obblighi e le responsabilità che la legge pone a loro carico nonché i compiti di ispezione, verifica e sorveglianza in materia di SSL.

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti.

#### **Il Datore di Lavoro**

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

- i) valutare tutti i rischi per la sicurezza e per la salute dei Lavoratori presso le varie sedi della Società;
- ii) elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi<sup>9</sup> (da custodirsi presso ciascuna sede e/o laboratorio) contenente tra l'altro:

---

<sup>9</sup> La valutazione dei rischi deve essere immediatamente rielaborata, in occasione di modifiche del processo produttivo o della organizzazione del lavoro significative ai fini della salute e sicurezza dei lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione o a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità.

- una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa; tali criteri devono essere caratterizzati da semplicità, brevità e comprensibilità, in modo da garantirne la completezza e l'idoneità quale strumento operativo;
- l'indicazione delle eventuali misure di prevenzione e di protezione attuate e degli eventuali dispositivi di protezione individuale adottati a seguito della suddetta valutazione dei rischi (articoli 74-79 del Testo Unico Sicurezza);
- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
- l'individuazione delle modalità di attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere;
- l'indicazione del nominativo del Delegato Sicurezza responsabile, qualora il Datore di Lavoro vi abbia provveduto, del RSPP, del RLS e del Medico Competente che abbiano partecipato con loro alla valutazione del rischio.

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il Delegato Sicurezza eventualmente nominato, RSPP e il Medico Competente.

La valutazione dei rischi è condivisa con il Rappresentante dei Lavoratori per la Sicurezza.

Nelle suddette ipotesi il DVR deve essere tempestivamente rielaborato rispetto all'accertamento dell'evento che determina l'esigenza modificativa.

iii) designare il Responsabile del Servizio di Prevenzione e Protezione.

Al Datore di Lavoro sono attribuiti numerosi altri compiti dallo stesso delegabili a soggetti qualificati. Tali compiti, previsti dal Testo Unico Sicurezza, riguardano, tra l'altro:

- la nomina del Medico Competente per l'effettuazione della Sorveglianza Sanitaria;
- la designazione preventivamente dei Lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione delle emergenze;
- l'adempimento degli obblighi di informazione, formazione ed addestramento;
- la convocazione della riunione periodica di cui all'articolo 35 del Testo Unico Sicurezza;
- l'aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi che hanno rilevanza ai fini della salute e sicurezza del lavoro, etc..

In relazione a tali compiti, ed a ogni altro compito affidato al Datore di Lavoro che possa essere da questi ultimi delegato ai sensi del Testo Unico Sicurezza, la suddetta delega è ammessa con i seguenti limiti e condizioni:



## DIGITAL SOLUTIONS

- che esso risulti da atto scritto recante data certa;
- che il delegato possenga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
- che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate.

Al fine di garantire l'attuazione di un modello di sicurezza aziendale sinergico e compartecipativo, il Datore di Lavoro fornisce al Servizio di Prevenzione e Protezione ed al Medico Competente informazioni in merito a:

- la natura dei rischi;
- l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
- la descrizione dei luoghi di lavoro e degli eventuali processi produttivi;
- i dati relativi agli infortuni e quelli relativi alle malattie professionali (*i.e.* schede relative alle attività svolte in sede o fuori sede).

Il Datore di Lavoro o, in caso di delega di funzioni, i suoi delegati, deve vigilare sull'adempimento degli obblighi che, in base alle disposizioni del Testo Unico Sicurezza, spettano a: i) preposti; ii) lavoratori; iii) progettisti; iv) fabbricanti; v) fornitori; vi) installatori; vii) medico competente.

### **I Delegati Sicurezza.**

I Delegati Sicurezza, qualora vengano nominati dal Datore di Lavoro, sono responsabili della salute e sicurezza sul lavoro, in ragione delle loro competenze professionali e dei poteri conferiti ai sensi dell'articolo 16 del Decreto Legislativo 81/2008, curano ed effettuano in piena autonomia i seguenti adempimenti:

- i) intrattengono relazioni con società terze a cui possono essere affidati adempimenti in materia di sicurezza;
- ii) si avvalgono della collaborazione del RSPP per la corretta gestione modalità di funzionamento del Servizio di Prevenzione e Protezione;
- iii) riferiscono al Datore di Lavoro, circa l'applicazione di procedure in materia di salute nei luoghi di lavoro;
- iv) accertano che il RSPP, il Medico Competente e il SPP abbiano predisposto i documenti previsti dall'articolo 30 del Decreto Legislativo 81/2008 e nel rispetto dei requisiti previsti dallo stesso articolo 30;
- v) si coordinano con il servizio di prevenzione e protezione per accertarsi, inoltre, che tali documenti siano idonei ad assicurare che:

## DIGITAL SOLUTIONS

- siano individuati i fattori di rischio, individuate le misure di sicurezza e salubrità degli ambienti di lavoro, nel rispetto della normativa vigente e sulla base della specifica conoscenza dell'organizzazione aziendale;
  - siano elaborate le misure preventive e protettive di cui all'articolo 28 del Testo Unico Sicurezza ed i sistemi di controllo di tali misure;
  - siano elaborate procedure di sicurezza e manutenzione e controllo per le varie attività aziendali;
- vi) collaborano con le varie funzioni aziendali, fornendo assistenza necessaria a garantire alla Società e il personale incaricato attuino le disposizioni impartite ed adempiano ai compiti assegnati;
- vii) si assicurano che il RSPP verifichi che:
- sia stata identificata ed applicata all'interno dei locali aziendali la segnaletica di sicurezza;
  - siano designati all'interno della struttura gli addetti e/o i preposti incaricati allo svolgimento delle attività inerenti la prevenzione e protezione;
  - siano stati effettivamente attuate tutte le misure tecniche ed organizzative suggerite dal RSPP, dall'SPP e dal Medico Competente, per ridurre al minimo i rischi connessi all'uso eventuale di attrezzature di lavoro;
  - siano stati consegnati ad ogni operatore i dispositivi di protezione individuale adeguati ai rischi connessi all'attività svolta secondo l'apposito organigramma funzionale (i.e. guanti e occhiali per la sostituzione dei *toner*);
  - sia stata data i) effettiva esecuzione ai provvedimenti indicati dal RSPP, dal SPP, dal Medico Competente, agli addetti al servizio di primo soccorso; ii) attuazione alle prescrizioni date dal RSPP per ovviare i rischi riscontrati in base alle valutazioni di cui al Decreto Legislativo 81/2008 tenendo conto della somma ovvero della combinazione dell'incidenza dei rischi; iii) attuazione alle misure preventive e protettive per singoli Lavoratori indicati dal Medico Competente sulla base delle risultanze degli esami da esso svolti;
- viii) verifica a consuntivo e in contraddittorio con RSPP l'efficacia delle disposizioni impartite.

Per l'esecuzione dell'incarico ai Delegati Sicurezza vengono conferiti, tra gli altri, i seguenti poteri:

- operare con tutti i poteri di organizzazione gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
- operare con l'autonomia di spesa necessaria per lo svolgimento delle funzioni delegate;
- utilizzare ai fini dell'esecuzione dell'incarico le risorse umane della Società nei limiti e secondo le modalità stabilite specificatamente nella delega.

### **Il Servizio di Prevenzione e Protezione (SPP).**

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro di Digital Solutions si avvalgono del Servizio di Prevenzione e Protezione dei rischi professionali che provvede:

- i) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- ii) ad elaborare, per quanto di competenza, le misure preventive e protettive a seguito della valutazione dei rischi e i sistemi di controllo di tali misure;
- iii) ad elaborare le procedure di sicurezza per le varie attività aziendali;
- iv) a proporre i programmi di informazione e formazione dei Lavoratori;
- v) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'articolo 35 del Testo Unico Sicurezza;
- vi) a fornire ai Lavoratori ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria.

Il RSPP provvede tra l'altro:

- i) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- ii) ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2 del Testo Unico Sicurezza e i sistemi di controllo di tali misure;
- iii) ad elaborare le procedure di sicurezza per le varie attività aziendali;
- iv) a proporre i programmi di informazione e formazione dei lavoratori;
- v) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35 del Testo Unico Sicurezza;
- v) a fornire ai lavoratori le informazioni di cui all'articolo 36 del Testo Unico Sicurezza.

I componenti del servizio di prevenzione e protezione sono tenuti al segreto in ordine ai processi lavorativi di cui vengono a conoscenza nell'esercizio delle proprie funzioni.

Qualora nell'espletamento delle attività di loro competenza, un RSPP della Società verificasse la sussistenza di eventuali criticità, (a titolo esemplificativo una situazione di pericolo grave ed imminente non risolta dal Datore di Lavoro) prescritte dal Datore di Lavoro, il RSPP coinvolto dovrà darne immediata comunicazione al Datore di Lavoro.

L'eventuale modifiche o sostituzione dei soggetti facenti parte del sistema di prevenzione e protezione dovrà essere comunicata tempestivamente all'OdV con l'espressa indicazione delle motivazioni a supporto di tale decisione.

Gli RSPP devono essere in possesso dei requisiti *ex* articolo 33 del Testo Unico Sicurezza.

### **Il Medico Competente.**

Il Medico Competente di Digital Solutions provvede tra l'altro a:

- i) collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della Sorveglianza Sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e dell'integrità psicofisica dei Lavoratori, all'attività di formazione ed informazione nei loro confronti, per la parte di competenza;
- ii) programmare ed effettuare la Sorveglianza Sanitaria;
- iii) istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ogni Lavoratore sottoposto a Sorveglianza Sanitaria;
- iv) fornire informazioni ai Lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informandoli sui relativi risultati;
- v) comunicare per iscritto in occasione della riunione periodica di cui all'articolo 35 del Testo Unico Sicurezza i risultati anonimi collettivi della Sorveglianza Sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica dei Lavoratori;
- vi) visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa in base alla valutazione di rischi.

Il Medico Competente deve essere in possesso di uno dei titoli *ex* articolo 38 del Testo Unico Sicurezza.

### **Il Rappresentante dei Lavoratori per la Sicurezza (RLS).**

È il soggetto eletto o designato, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i Lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro ed in ottemperanza all'articolo 47 del Testo Unico Sicurezza.

Difatti, in conformità a quanto previsto dal Decreto Legislativo 81/08 gli RLS di Digital Solutions ricevono, a cura del Datore di Lavoro o di un loro delegato, la formazione specifica in materia di salute e sicurezza.

RLS:

- i) accede ai luoghi di lavoro;
- ii) può richiedere consegna di copia del DVR e del DUVRI per finalità connesse all'espletamento dei compiti ad loro affidati;
- iii) è consultato preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- iv) è informati in merito all'organizzazione delle attività formative;

## DIGITAL SOLUTIONS

- v) promuove l'elaborazione, l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei Lavoratori;
- vi) partecipa alla riunione periodica di cui all'articolo 35 del Decreto Legislativo 81/08;
- vii) è informato in merito alla valutazione dei rischi e le misure di prevenzione relative e, ove ne faccia richiesta e per l'espletamento della loro funzione, copia del Documento di Valutazione dei Rischi e del DUVRI.

RLS, se risorsa interna, dispone del tempo necessario allo svolgimento dell'incarico, senza perdita di retribuzione, nonché dei mezzi necessari per l'esercizio delle funzioni e delle facoltà riconosciute; non possono subire alcun pregiudizio a causa dello svolgimento della propria attività e nei loro confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.

### **I Lavoratori.**

Secondo quanto previsto all'articolo 20 del Decreto Legislativo 81/2008, i Lavoratori sono sottoposti a determinati obblighi tra cui:

- i) prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal Datore di Lavoro;

I Lavoratori devono in particolare:

- i) contribuire, insieme al Datore di Lavoro, ai delegati e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
- ii) osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai delegati e dai preposti, ai fini della protezione collettiva ed individuale;
- iii) utilizzare correttamente le attrezzature di lavoro;
- iv) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
- v) segnalare immediatamente le deficienze dei mezzi e dei dispositivi di cui sono dotati nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli e fatto salvo l'obbligo di non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- vi) eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al RLS;
- vii) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- viii) non compiere di propria iniziativa operazioni o manovre che non sono di propria competenza ovvero che possono compromettere la sicurezza propria o di altri Lavoratori;
- ix) partecipare ai programmi di formazione e di addestramento;
- x) sottoporsi ai controlli sanitari previsti dal presente Testo Unico Sicurezza o comunque disposti dal Medico Competente.

## DIGITAL SOLUTIONS

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

I lavoratori di aziende che svolgono per la Società attività in regime di appalto e subappalto devono essere riconoscibili ed esporre apposita tessera di riconoscimento.

### **d. Informazione e formazione.**

#### **Informazione.**

Il contenuto della informazione che Digital Solutions riserva ai Lavoratori deve essere facilmente comprensibile e deve consentire agli stessi di acquisire le relative conoscenze e la necessaria consapevolezza in merito a:

- i) le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle regole adottate dalla Società in tema di SSL;
- ii) il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di sicurezza e ogni altra prescrizione relativa al sistema di SSL adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale;
- iii) in caso di trasferte, informazioni puntuali, in relazione al grado di rischio, incluse le azioni da intraprendere in caso di pericolo.

Ciò premesso, la Società, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun Lavoratore, è tenuta ai seguenti oneri informativi:

- i) la Società deve fornire adeguata informazione ai dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti) circa i rischi specifici dell'impresa, per quanto limitati, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;
- ii) deve essere data evidenza dell'informativa erogata per la gestione del primo soccorso, emergenza, evacuazione e prevenzione incendi e devono essere verbalizzati gli eventuali incontri;
- iii) i Dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti) devono ricevere informazione sulla nomina dei vari responsabili della sicurezza nominati presso la Società tra cui, a solo fine esemplificativo, del RSPP, del Medico Competente e sugli addetti ai compiti specifici per il primo soccorso, lotta antincendio, evacuazione dai luoghi di lavoro;
- iv) deve essere formalmente documentata l'informazione e l'istruzione per l'uso delle attrezzature di lavoro messe a disposizione dei Lavoratori;
- v) il servizio di Formazione e Protezione è coinvolto nel processo di informazione dei lavoratori.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita registrazione presso i servizi prevenzione e protezione.

### Formazione.

- i) La Società come previsto all'articolo 37 del Testo Unico Sicurezza deve fornire adeguata formazione a tutti i Lavoratori in materia di salute e sicurezza sul lavoro anche rispetto alle conoscenze linguistiche del Lavoratore. L'attività di formazione deve essere ripetuta periodicamente;
- ii) il servizio di prevenzione protezione collabora con il Datore di Lavoro alla stesura del piano di formazione sulla base dei contenuti minimi e delle modalità, definiti dagli accordi presi in sede di conferenza permanente Stato-Regioni;
- iii) in caso di trasferte, in relazione al grado di rischio, i lavoratori vengono formati in merito ai rischi incluse le azioni da intraprendere in caso di pericolo;
- iv) la formazione erogata deve prevedere questionari di valutazione e verifica dell'apprendimento;
- v) la formazione deve essere adeguata ai rischi della mansione cui il Lavoratore è in concreto assegnato;
- vi) i rappresentanti dei Lavoratori per la sicurezza hanno diritto ad una formazione specifica in materia di salute e sicurezza;
- vii) gli addetti a specifiche mansioni all'interno dell'azienda (*i.e.* utilizzo di strumenti, agenti chimici etc.) e/o specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al primo soccorso) devono ricevere specifica formazione;
- viii) Digital Solutions deve effettuare periodiche esercitazioni di evacuazione di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze).

Pertanto, i Lavoratori, i preposti ed i dirigenti per la sicurezza ricevono a cura del Datore di Lavoro, un'adeguata e specifica formazione e un aggiornamento periodico in relazione ai propri compiti in materia di SSL.

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione e conservazione anche sulla *intranet* aziendale.

### e. Comunicazione, flusso informativo e cooperazione.

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, la Società si organizza per garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Lavoratori.

A tal proposito la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

- *dal basso verso l'alto.*

Il flusso dal basso verso l'alto è garantito dalla Società mettendo a disposizione apposite schede di segnalazione attraverso la compilazione delle quali ciascuno dei Lavoratori ha la possibilità di portare a conoscenza del proprio superiore gerarchico osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale;

## DIGITAL SOLUTIONS

- dall'alto verso il basso.

Il flusso dall'alto verso il basso ha lo scopo di diffondere a tutti i Lavoratori la conoscenza del sistema adottato dalla Società per la gestione della sicurezza nel luogo di lavoro.

A tale scopo la Società garantisce ai Destinatari, anche attraverso l'*intranet* aziendale, un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- i) eventuali nuovi rischi in materia di salute e sicurezza dei Lavoratori;
- ii) modifiche nella struttura organizzativa adottata dalla Società per la gestione della salute e sicurezza dei Lavoratori;
- iii) contenuti delle procedure aziendali adottate per la gestione della sicurezza e salute dei Lavoratori;
- iv) ogni altro aspetto inerente alla salute e alla sicurezza dei Lavoratori.

### **f. Documentazione.**

La Società dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, i seguenti documenti:

- i) la cartella sanitaria, la quale deve essere istituita, gestita e aggiornata esclusivamente dal Medico Competente, custodita secondo le modalità concordate con il Datore di Lavoro e conservata per 10 anni;
- ii) i Documenti di Valutazione dei Rischi che indicano la metodologia con la quale si è proceduto alla valutazione dei rischi e contenenti il programma delle misure di mantenimento e di miglioramento.

La Società è altresì chiamata a garantire che:

- i) RSPP, il Medico Competente, i delegati, gli incaricati dell'attuazione delle misure di emergenza e primo soccorso, vengano nominati formalmente e tali nomine siano costantemente aggiornate;
- ii) venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente da RSPP e dal Medico Competente;
- iii) vengano adottati e mantenuti aggiornati i registri delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica;
- iv) venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale;
- v) vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature ed eventuali dispositivi di protezione individuale forniti dai costruttori;
- vi) venga conservata ogni procedura adottata dalla Società per la gestione della salute e sicurezza sui luoghi di lavoro;



## DIGITAL SOLUTIONS

vii) tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'OdV.

### **g. L'attività di monitoraggio.**

La Società deve assicurare un costante ed efficace monitoraggio delle misure di prevenzione e protezione adottate sui luoghi di lavoro.

A tale scopo la Società:

- i) assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- ii) assicura un costante monitoraggio dell'adeguatezza e della funzionalità di tali misure per il raggiungimento degli obiettivi prefissati e della loro corretta applicazione;
- iii) compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere.

Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta, la Società, si avvale del servizio di prevenzione e protezione che laddove la specificità del campo di intervento lo richiedesse, potrà fare affidamento anche a risorse esterne con elevato livello di specializzazione.

La Società garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.

Inoltre, con riferimento alla *security* per i lavoratori che svolgono trasferte all'estero, la Società ha implementato un sistema per l'autorizzazione trasferte, che prevede una mappatura puntuale dei paesi in funzione dei differenti parametri relativi al rischio.

### **h. Il riesame del sistema.**

Al termine dell'attività di monitoraggio di cui alla precedente paragrafo, il sistema adottato dalla Società per la gestione della salute e sicurezza dei lavoratori è sottoposto ad un riesame periodico da parte della Società, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.

## **F.5 Presidi in tema di sicurezza e selezione ed assunzione del personale.**

### **F.5.1. Principi generali di comportamento.**

La politica della Società deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società nonché il rispetto del Testo Unico della Sicurezza.

Tale politica deve contenere:

- i) una chiara affermazione della responsabilità dell'intera organizzazione aziendale, dal Datore di Lavoro al singolo Lavoratore, nella gestione delle tematiche relative sia alla salute e sicurezza sul lavoro sia alla selezione e assunzione del personale, ciascuno per le proprie attribuzioni e competenze;

## DIGITAL SOLUTIONS

- ii) l'impegno a considerare tali tematiche come parte integrante della gestione aziendale;
- iii) l'impegno al miglioramento continuo ed alla prevenzione;
- iv) l'impegno a fornire le risorse umane e strumentali necessarie;
- v) l'impegno a garantire che i Destinatari, nei limiti delle rispettive attribuzioni, siano sensibilizzati a svolgere la propria attività nel rispetto delle norme sulla tutela della salute e sicurezza;
- vi) l'impegno al coinvolgimento ed alla consultazione dei Lavoratori, anche attraverso RLS;
- vii) l'impegno ad un riesame periodico della politica per la salute e sicurezza o verifica delle assunzioni al fine di garantire la sua costante adeguatezza alla struttura organizzativa della Società.

### **F.5.2. Principi Specifici di comportamento - I contratti di appalto con specifico riferimento all'assunzione di mano d'opera.**

Stante i presidi adottati con riferimento alla politica aziendale per la sicurezza nei luoghi di lavoro ed il SSL, la attività relative alla selezione delle controparti destinate a fornire specifici servizi (quali ad esempio le imprese con alta incidenza di manodopera non qualificata) deve essere svolta con particolare attenzione e in base ad apposite procedure interne.

In particolare, l'affidabilità di dette controparti deve essere valutata, ai fini della prevenzione dei Reati di cui alla presente Parte Speciale, anche attraverso specifiche verifiche *ex ante*.

Nei contratti con soggetti terzi con cui la Società collabora (Fornitori, Consulenti, etc.), deve essere contenuta apposita dichiarazione in cui la controparte garantisca, nel caso in cui siano previste attività in favore della Società, il rispetto della normativa italiana tempo per tempo vigente in materia di lavoro irregolare, con la previsione del diritto di Digital Solutions alla risoluzione del contratto (con eventuale pagamento di penali) in caso di inadempimento.

Tale dichiarazione è consigliabile sia rinnovata periodicamente (su base annuale) nel caso di contratti di durata superiore ad un anno. Detti contratti dovranno essere accompagnati dall'elenco del personale impiegato e tempestivamente aggiornati in caso di variazioni.

La Società deve predisporre e mantenere aggiornato l'elenco delle aziende che operano all'interno del proprio sito con contratto d'appalto.

La Società predisporre idonee procedure di accesso al proprio perimetro aziendale, al fine di garantire l'identificazione del personale di società terze svolgenti prestazioni a carattere continuativo per la stessa (es. obbligo di esposizione del cartellino di riconoscimento provvisto di fotografia e indicazione dell'impresa di appartenenza).

Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti di cui all'articolo 26 del Testo Unico Sicurezza, tra questi, in capo al Datore di Lavoro:

- i) verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori, ai servizi e alle forniture da affidare in appalto attraverso: (i) acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato; (ii) acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei

## DIGITAL SOLUTIONS

requisiti di idoneità tecnico professionale ai sensi dell'articolo 4, D.P.R. 28 dicembre 2000, n. 445;

- ii) fornire informazioni dettagliate agli appaltatori circa gli eventuali rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- iii) cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro e incidenti sull'attività lavorativa oggetto dell'appalto;
- iv) coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i Lavoratori;
- v) predisporre un unico DUVRI che indichi le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva; tale documento deve allegarsi al contratto di appalto o d'opera; il DUVRI dovrà essere prontamente adeguato all'evoluzione dei servizi e dei lavori.

Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze delle lavorazioni. A tali dati possono accedere, su richiesta, i Rappresentanti per la Sicurezza dei Lavoratori.

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

L'imprenditore committente risponde in solido con l'appaltatore, nonché con ciascuno degli eventuali ulteriori subappaltatori, per tutti i danni per i quali il lavoratore, dipendente dall'appaltatore o dal subappaltatore, non risulti indennizzato ad opera dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro.

**PARTE SPECIALE G**

**REATI TRIBUTARI**

*Articolo 25-quinquiesdecies del Decreto Legislativo 231/2001*

# DIGITAL SOLUTIONS

## G.1 Funzione della Parte Speciale G.

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i Destinatari del Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato richiamate dall'articolo 25-*quinquiesdecies* del Decreto Legislativo 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di:

- c) definire le procedure che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- d) supportare l'Organismo di Vigilanza e i responsabili delle altre funzioni aziendali ad esercitare le attività di controllo, monitoraggio e verifica.

## G.2 Fattispecie di Reato rilevanti.

Per completezza, di seguito vengono riportate tutte le fattispecie di reato che fondano la responsabilità amministrativa degli enti ai sensi dell'art. 25-*quinquies* del Decreto.

### G.2.1 Delitti di tributari

#### **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. 74/2000).**

Il reato punisce chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in dichiarazione elementi fittizi.

#### **Dichiarazione fraudolenta mediante altri artifici (art. 3 D.lgs. 74/2000).**

Il reato punisce chi, fuori dai casi previsti dall'art. 2, compiendo operazioni simulate oggettivamente o soggettivamente o avvalendosi di documenti falsi o altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica nelle dichiarazioni di cui sopra elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizie quando congiuntamente l'imposta evasa, con riferimento alla singola imposta, è superiore ad € 30.000 e l'ammontare complessivo degli elementi attivi sottratti all'imposizione, è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o comunque superiore a € 1.500.000, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in riduzione dell'imposta è superiore al 5% dell'ammontare dell'imposta medesima o comunque a € 30.000.

#### **Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs. 74/2000).**

Il reato punisce chi, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

#### **Occultamento o distruzione di documenti contabili (art. 10 D.lgs. 74/2000).**

Il reato punisce chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume d'affari.

### **Sottrazione fraudolenta al pagamento di imposte (art. 11 D.lgs. 74/2000).**

Il reato punisce chi, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad € 50.000, aliena simulatamente o compie atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficacie la procedura di riscossione coattiva. Inoltre chi, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad € 50.000.

A seguito delle modifiche apportate dal Decreto Legislativo n. 75 del 14 luglio 2020, qualora siano commessi nell'ambito di sistemi fraudolenti transfrontalieri ed al fine di evadere l'IVA per un importo complessivo non inferiore a dieci milioni di euro, sono inclusi quali reati presupposto anche i seguenti delitti previsti dal d.l. 74/2000:

### **Dichiarazione infedele (art. 4 D.lgs. 74/2000)**

Il reato punisce chi, al fine di evadere le imposte sui redditi o l'iva, indica in una delle relative dichiarazioni annuali elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando congiuntamente l'imposta evasa è superiore, con riferimento a taluna, ad € 150.000 e l'ammontare complessivo degli elementi attivi sottratti all'imposizione è superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o è comunque superiore ad € 3.000.000

### **Omessa dichiarazione (art. 5 D.lgs. 74/2000)**

Il reato punisce chi, al fine di evadere le imposte sui redditi o l'iva, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore ad € 50.000, anche con riferimento alla dichiarazione di sostituto d'imposta

### **Indebita compensazione (art. 10<sup>quater</sup> D.lgs. 74/2000)**

Il reato punisce chi non versa le somme dovute utilizzando in compensazione crediti non spettanti o inesistenti per un importo annuo superiore ad € 50.000.

## **G.3 Aree di rischio ed Attività Sensibili.**

Le Aree di Rischio della Società, con riferimento ai delitti tributari, sono riconducibili a:

- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*
- *Gestione dei flussi finanziari e predisposizione delle scritture contabili;*
- *Selezione e gestione di segnalatori, sviluppatori e partner commerciali;*
- *Gestione dei rapporti con società di certificazione e con il revisore.*

## DIGITAL SOLUTIONS

### G.4 Principi generali di comportamento.

Obiettivo del presente capitolo è che i Destinatari si attengano, nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento delle Attività Sensibili, individuate nella presente Parte Speciale, a regole di condotta conformi a quanto qui prescritto, oltre al rispetto del Codice Etico e delle *policy* aziendali.

In particolare, la Società adotta i seguenti principi generali, a cui i Destinatari devono attenersi:

- i) la segregazione dei ruoli;
- j) la valutazione comparativa di più offerte contrattuali, salvo deroghe disciplinate da apposite procedure aziendali;
- k) la formalizzazione e tracciabilità degli acquisti dall'attivazione alla fine;
- l) la verifica della congruità dei corrispettivi negoziati ed attività svolte;
- m) la forma scritta dell'accordo e l'indicazione nello stesso del compenso pattuito o delle modalità con cui determinare lo stesso;
- n) l'adozione di modalità di pagamento che escludano l'utilizzo di conti non intestati al consulente/fornitore e, in ogni caso, escludano pagamenti in contanti;
- o) la predisposizione di albo fornitori ovvero di apposite liste di consulenti e di fornitori già preventivamente qualificati e la cui presenza nell'albo viene periodicamente rivalutata;
- p) l'inserimento nei contratti di clausole che impegnino i consulenti e i fornitori, nella conduzione dei propri affari e nella gestione dei rapporti con terzi, a riferirsi a principi equivalenti a quelli adottati da Digital Solutions in materia di corruzione e contemplino il diritto della Società alla risoluzione del contratto (con eventuale pagamento di penali).

Inoltre la Società deve provvedere a:

- f) instaurare rapporti esclusivamente con controparti che godano di una comprovata reputazione e rispettabilità e la cui cultura etica aziendale sia comparabile a quella della Società;
- g) assicurare la trasparenza degli accordi ed evitare la sottoscrizione di patti o accordi contrari alla legge;
- h) mantenere con le controparti rapporti trasparenti e collaborativi;
- i) segnalare tempestivamente all'OdV ogni comportamento della controparte che appaia contrario ai principi etici di cui al Codice Etico;
- j) gestione trasparente degli acquisti di beni e servizi, dei flussi finanziarie dei rapporti *inter-company*.

### G.5 Principi specifici di comportamento.

Per i principi specifici di comportamento relativi alle seguenti Attività Sensibili, ovvero:

- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*

## DIGITAL SOLUTIONS

- *Gestione dei flussi finanziari e predisposizione delle scritture contabili;*
- *Selezione e gestione di segnalatori, sviluppatori e partner commerciali*

si rinvia a quanto previsto nella Parte Speciale A “*Reati commessi nei rapporti con la Pubblica Amministrazione e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria*” nella Parte Speciale B “*Reati Societari*” e nella Parte Speciale C “*Reati di corruzione tra privati*”