



MODELLO ORGANIZZATIVO DI GESTIONE E CONTROLLO ai sensi del D.Lgs. 231/2001 (estratto)

Numero revisione	Descrizione revisione	Redatto da	Data approvazione del C.d.A.
0	Prima Stesura	Roberto Conforto (C.E.O.)	18 dicembre 2017
1	Prima Revisione	Roberto Conforto (C.E.O.)	15 gennaio 2019

MODELLO ORGANIZZATIVO DI GESTIONE E CONTROLLO: PARTE GENERALE

INTRODUZIONE

Il decreto legislativo 8 Giugno 2001 n°231 ha introdotto nel nostro ordinamento la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica. In base a tale normativa, nel caso in cui vengano commessi i reati previsti nel decreto la Società può essere ritenuta direttamente responsabile, a meno che non dimostri di avere adottato un modello di organizzazione, di gestione e di controllo tale per cui l'azione sia stata commessa intenzionalmente in violazione alle disposizioni aziendali.

Computer Solutions® S.P.A. ha deciso di dotarsi di un Modello Organizzativo di Gestione e Controllo, con delibera del Consiglio di Amministrazione del 18 Maggio 2012.

Computer Solutions® S.P.A. confida sul comportamento di tutti i propri dipendenti e collaboratori per mantenere un corretto livello di applicazione delle disposizioni previste dal presente Modello Organizzativo.

Il mancato rispetto (in tutto o in parte) delle disposizioni definite nel presente Modello Organizzativo, sarà considerato da Computer Solutions® S.P.A. come motivo per determinare appropriate sanzioni disciplinari nei confronti di chi ha commesso il reato.

Il presente documento costituisce e descrive il Modello Organizzativo per la prevenzione dei reati previsti nel decreto. L'obiettivo è quello di integrare le norme di condotta, i principi e tutti gli strumenti organizzativi e di controllo esistenti per la corretta applicazione delle norme.

Per prevenire il rischio di commissione di reati dai quali possa derivare la responsabilità dell'Impresa ai sensi del D.Lgs. n. 231/2001, il Modello prevede:

- l'individuazione delle attività nel cui ambito possono essere commessi reati;
- specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Impresa in relazione ai reati da prevenire;
- l'individuazione di modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello;
- l'introduzione di un sistema disciplinare, in coerenza col regolamento interno, idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

In particolare, adottando il modello organizzativo Computer Solutions® S.P.A. intende:

- rendere consapevoli tutti coloro che operano per e nome e per conto della Società dei possibili reati in cui possono incorrere e delle conseguenze sanzionatorie e disciplinari.
- riaffermare che comportamenti difformi ai dettami del Codice Etico sono fortemente condannati dalla Società.
- vigilare sulle attività a rischio per prevenire e contrastare il verificarsi dei reati.
- Il modello deve essere conosciuto e rispettato da tutto il personale della Società, nello specifico:
 - Amministratori e Sindaci
 - personale, inclusi i dipendenti, che opera per nome e per conto della società
 - lavoratori parasubordinati

La Società impone il rispetto delle norme e dei comportamenti anche a collaboratori terzi (fornitori, consulenti ecc.) tramite precise clausole contrattuali che prevedano la risoluzione del contratto in caso di violazione.

LA COSTRUZIONE DEL MODELLO ORGANIZZATIVO

La predisposizione del presente Modello Organizzativo è stata preceduta da una serie di attività preparatorie suddivise in differenti fasi e dirette tutte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D. Lgs. 231/2001.

Si descrivono qui di seguito le fasi che hanno permesso la predisposizione del presente Modello.

Fase preliminare: in tale fase, finalizzata alla predisposizione della documentazione di supporto ed alla pianificazione delle attività di rilevazione, in collaborazione col CEO, sono state condotte analisi puntuali sulla documentazione esistente (organigramma, qualità, processi, rilevazioni e controlli) e confronti con le funzioni aziendali interessate, allo scopo di identificare i soggetti da intervistare e coinvolgere nella successiva fase di valutazione dei rischi e del sistema dei controlli.

Inoltre, sono state individuate le aree di attività (ambiti societari, ambiti organizzativi, processi operativi) nelle quali esiste il rischio di commissione dei reati previsti dal D. Lgs. 231/2001 e, allo scopo di facilitare la successiva fase di valutazione dei rischi, sono state identificate le possibili modalità di conduzione della condotta illecita.

Fase di mappatura rischi e controlli: in tale fase è stata effettuata un'approfondita indagine dell'organizzazione di Computer Solutions, ovvero una ricognizione delle aree, delle relative funzioni e procedure e delle entità esterne, in vario modo correlate con la Società.

Per ciascuna di tali aree sono state condotte analisi documentali e interviste ai soggetti coinvolti nelle attività esaminate, per identificare i reati potenzialmente commisibili, le concrete modalità di commissione, la natura dei controlli esistenti e la loro efficacia. Nel dettaglio si è proceduto a:

- identificare l'operatività" adottata dalla Società in merito ai cosiddetti processi "sensibili";
- descrivere le posizioni e i soggetti coinvolti, le loro responsabilità ed i loro poteri;
- identificare e descrivere i reati commisibili e le conseguenze che essi potrebbero avere;
- individuare e descrivere la possibile condotta illecita propria dell'attività in esame e le modalità pratiche attraverso cui i reati potrebbero essere commessi;
- stimare la frequenza con la quale, nella normale operatività aziendale, si svolgono le attività in esame e dunque con quale frequenza si possano presentare occasioni di commissione dei reati individuati;
- individuare in maniera puntuale i controlli esistenti e valutare l'allineamento della struttura di controllo ai dettami del D. Lgs. 231/2001 in termini di esistenza, efficacia ed efficienza dei controlli, esistenza di procedure formalizzate, adeguatezza del sistema delle deleghe e procure, esistenza e adeguatezza del sistema disciplinare.

La fase di rilevazione dei rischi e dei controlli ha consentito di pervenire alla ricostruzione di dettaglio delle aree aziendali "sensibili", con identificazione delle funzioni e dei soggetti coinvolti e della loro responsabilità nonché dei sistemi di controllo adottati per la mitigazione dei rischi.

Fase di valutazione rischi e controlli: in tale fase, in collaborazione col CEO, si è provveduto, per ciascuno dei processi sensibili, alla valutazione del grado di rischiosità:

- per ciascun processo è stato valutato il rischio che vengano commessi illeciti amministrativi dipendenti da reato, tenuto conto del grado di efficacia e di efficienza delle procedure e dei sistemi di controllo esistenti all'interno del processo, in quanto idonei a valere anche come misure di prevenzione dei reati;
- sulla base di dette valutazioni è stato determinato il livello di criticità, sotto il profilo del rischio ai sensi del D. Lgs. 231/2001, nell'ambito di ciascun processo identificato;

in relazione alle aree di rischio identificate sono state individuate le opportune azioni correttive per migliorare il sistema dei controlli e ridurre il livello di criticità.

DEFINIZIONI E GLOSSARIO

I seguenti termini usati nel Modello Organizzativo avranno il corrispondente significato:	
Amministrazione e finanza	Si intende l'Area aziendale che svolge tutte le funzioni di amministrazione e finanza per Computer Solutions S.P.A.
Analisi dei rischi	Si tratta del processo di valutazione dei rischi aziendali.
Area aziendale	Si intende un settore aziendale che può comprendere una o più Funzioni aziendali.
ATI / RTI	Si intende l'associazione temporanea d'impresе o il raggruppamento temporaneo d'impresе finalizzati alla partecipazione a gare d'appalto pubbliche o alla stipulazione di contratti di appalto tra privati.
Attività aziendale	Si intende l'ordinaria operazione aziendale svolta nell'ambito delle mansioni attribuite alla specifica Funzione aziendale.
Attività sensibile o Processo sensibile	Si intende un'operazione o una serie di operazioni svolte ordinariamente dal personale dipendente nell'ambito delle proprie mansioni e che, per la loro caratteristica, richiedono l'applicazione di specifici controlli al fine di limitare l'esposizione al rischio di commissione dei reati previsti dal Decreto.
Chief Executive Officer (C.E.O.)	Si intende l'Amministratore Delegato
Chief Financial Officer (C.F.O.)	Si intende il Direttore Finanziario o organismo facente funzioni
Codice Etico	Indica i principi etici della Società finalizzati ad evitare comportamenti che possono comportare le fattispecie di reato previste dal Decreto.
Collaboratore	Si intende il soggetto esterno alla Società che svolge un'attività lavorativa a tempo determinato per l'azienda in base a specifico contratto regolamentato dalla legge.
Collegio Sindacale	Si intende il collegio sindacale in carica della Società.
Compliance	Si intende l'insieme delle procedure e dei controlli (prevalentemente finanziari) per garantire conformità a leggi o regolamenti.
Consiglieri del Consiglio di Amministrazione	Si intendono gli amministratori in carica della Società.
Consiglio di Amministrazione (C.d.A.)	Si intende il consiglio di amministrazione della Società.
Consulente	Si intende il soggetto esterno alla Società che svolge un'attività professionale non continuativa ed in piena autonomia a favore della stessa in base a specifico accordo contrattuale.
Controllo (interno)	Si intende l'insieme delle Procedure aziendali poste in essere dai Consiglieri per garantire la corretta esecuzione delle Attività aziendali, l'affidabilità, l'accuratezza e la completezza delle informazioni, nonché la salvaguardia del patrimonio aziendale.
Decreto	Indica il Decreto Legislativo 8 Giugno 2001 n° 231 e successive modificazioni e integrazioni.
Direttori/Dirigenti	Si intendono il lavoratori preposti alla direzione di una o più Aree aziendali con autonomia decisionale a cui compete promuovere, gestire e coordinare la realizzazione degli obiettivi aziendali.
Documento di valutazione dei rischi aziendali	Si intende il documento di cui agli artt. 17 e 28 del D.Lgs. 81/08.
Documento programmatico sulla sicurezza	Si intende il documento redatto in base alle disposizioni di cui al punto 19 del disciplinare tecnico in materia di misure minime di sicurezza, allegato b del D.Lgs. n. 196 del 30 giugno 2003.

Forecast	Modelli di previsione.
Gestione del Personale (HR)	Si intende l'Area aziendale che cura la gestione del personale ed il sistema assuntivo.
Information Technology (IT)	Settore specialistico riferito all'informatica.
Legale	Si intende l'Area aziendale che cura gli aspetti giuridici connessi all'Attività aziendale.
Linee Guida di Confindustria	Si tratta delle linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del Decreto, approvate il 7 marzo 2002 (aggiornate al 31 marzo 2008).
Medico Competente (MC)	Il Medico Competente collabora con il datore di lavoro per effettuare la sorveglianza sanitaria ai sensi del Testo Unico in materia di salute e sicurezza sul lavoro
Modello Organizzativo (MOG)	Indica il modello di organizzazione, gestione e controllo idoneo a prevenire i reati predisposto dalla Società ai sensi del D.Lgs. 231/2001.
Organigramma	Si intende il sistema di rappresentazione delle varie funzioni aziendali organizzate per lo svolgimento dell'Attività aziendale secondo i relativi rapporti gerarchici intercorrenti.
Organismo di vigilanza (O.d.V.)	L'organismo dotato di autonomi poteri di iniziativa e di controllo di cui all'art. 6 del Decreto nominato dalla Società.
Policy	Si intende l'insieme di regole, direttive e principi stabiliti per la gestione aziendale che sono anche indirizzate, direttamente o indirettamente, alla prevenzione della commissione dei reati di cui al Decreto.
Procedura	Un'insieme di regole aziendali codificate e da applicare nello svolgimento di una specifica Attività aziendale svolta da una Funzione aziendale incluse le Policies e i Protocolli.
Processo	Si intende l'insieme di attività interrelate o interagenti che descrivono il percorso di specifiche Attività aziendali trasformando le risorse in prodotto, sia esso un bene, un servizio o un'informazione o una combinazione di tali elementi. Il processo aziendale può coinvolgere diverse Aree aziendali o Funzioni aziendali.
Project Manager (Responsabile di commessa)	Ruolo aziendale riferito al soggetto che opera all'interno delle Business Unit e preposto alla gestione delle attività di erogazione dei servizi ai clienti.
Protocolli o Controlli preventivi	Si intendono le regole di controllo previste nello svolgimento di un'Attività aziendale e finalizzati a contrastare i rischi di commissione dei reati di cui al Decreto.
Pubblica Amministrazione (P.A.)	Si intende quanto previsto al paragrafo 3.1.1 della Parte "A" – Reati contro la Pubblica Amministrazione all'interno della Parte Speciale del presente Modello Organizzativo.
Quality Manager	Ruolo aziendale riferito al soggetto che opera nell'ambito del controllo di qualità come indicato nell'Organigramma.
Ricerca e Sviluppo (R&S)	Si intendono le Attività di Ricerca e Sviluppo svolte in azienda
Selezione del Personale	Si intende l'attività svolta nell'ambito dell'Area aziendale di Gestione del Personale che cura il sistema assuntivo del personale dipendente.

Regolamento	Regolamento di funzionamento dell'Organismo di vigilanza predisposto dal medesimo.
Responsabile dei sistemi informativi	Il responsabile dei sistemi informativi è una figura professionale incaricata della gestione e manutenzione degli impianti di elaborazione con cui vengono trattati i dati personali, compresi i gestionali data base, i sistemi software complessi, i network e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali
Responsabile dell'Area aziendale	Si intendono i soggetti a cui è affidata la responsabilità di una specifica Area aziendale come descritte nell'Organigramma (nell'ambito delle Business Unit indicate).
Responsabile di Funzione aziendale	Si intende il soggetto a cui è affidata la responsabilità di una specifica Funzione aziendale inseriti all'interno delle singole Unità Organizzative e delle Aree aziendali che compongono l'Organigramma.
Responsabile della Privacy	Si intende la persona preposta dal titolare del trattamento dei dati personali in base all'art. 29 del del D.Lgs. n. 196 del 30 giugno 2003.
Responsabile di Unità Organizzativa oppure della Business Unit	Si intende il soggetto al quale è attribuito il ruolo di supervisione, gestione e controllo di un'Unità Organizzativa.
R.S.P.P.	Si tratta del responsabile del servizio di prevenzione e protezione di cui all'art. 2 lett. f) del TU.
RTI	Si intende il raggruppamento temporaneo d'impresе finalizzato alla partecipazione a gare d'appalto pubbliche o alla stipulazione di contratti di appalto tra privati.
Sindaci	Si intendono i sindaci in carica della Società.
Sistema disciplinare	Si intende il sistema disciplinare di cui agli artt. 6 e 7 del Decreto idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo.
Software	Insieme di programmi per computer creati allo scopo di gestire problematiche specifiche.
Soggetti destinatari	Sono i soggetti sia dipendenti che terzi rispetto alla Società ai quali sono indirizzati i principi etici, le istruzioni operative ed il Modello Organizzativo nel suo insieme, ciascuno secondo i livelli di responsabilità a loro attribuiti.
System integration	Integrazione tra sistemi.
TARI	Tariffa Rifiuti
TARSU	Tassa Asporto Rifiuti Solidi Urbani
Testo Unico in materia di salute e sicurezza sul lavoro	Si intende il D.Lgs. n. 81/2008 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro".

PRESENTAZIONE DELL'AZIENDA

BREVE STORIA DELLA SOCIETÀ



Computer Solutions® S.p.A nasce nel 1988 con la *mission* di produrre software gestionale e servizi dedicati alla *gestione amministrativa dello smaltimento dei rifiuti*. La Società nasce dalle diverse esperienze di quattro professionisti della *information and communication technology*, esperienze maturate in settori complementari rivelatisi strategici per lo sviluppo dell'azienda.

L'inserimento di Computer Solutions® S.p.A. nel mercato è avvenuto con la costruzione e con la successiva commercializzazione di una linea di prodotti denominata Progetto Sma.R.T.® evoluto dal 2002 in Progetto Win Sm@.R.T.® e dal 2012 in



Nel tempo al prodotto core si sono aggiunti altri prodotti a marchi registrati quali TRACE®, SISgate® e Complia®. L'ingegnerizzazione e la pacchettizzazione dei diversi moduli che compongono Progetto Win Sm@.R.T.® sono specificatamente rivolti a risolvere le problematiche che gli operatori del settore dello smaltimento e del recupero si trovano ad affrontare nello svolgimento della loro attività, soprattutto per quanto riguarda il rispetto dei vincoli e degli obblighi imposti dalle normative vigenti ma anche sotto le prospettive organizzative, economiche, di sintesi manageriale, nonché, di controllo di processo. Nel corso del 2015 lo sforzo di sviluppo evolutivo di tutta la linea di prodotti si è concentrato, conseguentemente alla riduzione della platea dei soggetti obbligati all'adozione del SISTRI¹, sullo sfruttamento delle tecnologie web che permettono di attivare servizi collaborativi tra i nostri clienti/utenti, nonché, nello sfruttamento di tali tecnologie in progetti evolutivi sia dell'ampliamento dell'offerta sia del posizionamento nel mercato di Computer Solutions® S.p.A.

In ventisette anni di mercato Computer Solutions® S.p.A. ha saputo espandere la presenza dei propri prodotti su tutto il territorio nazionale, facendo crescere, di conseguenza, anche le risorse dedicate alla gestione ed al mantenimento della crescita.

Attualmente Computer Solutions® S.p.A. è da considerare azienda leader in Italia per la produzione e la commercializzazione di software specialistico dedicato alla gestione dello smaltimento/recupero dei rifiuti.

DESCRIZIONE DEI PRODOTTI

Progetto Win Sm@.R.T.® nasce nel paese, l'Italia, ove viene applicata la più complessa normativa esistente in Europa per la gestione ed il controllo dello smaltimento e del recupero dei rifiuti (sia urbani che industriali). Pertanto, il prodotto risulta tarato in modo nativo per affrontare ogni funzionalità possibile per risolvere il problema di adattabilità alle normative di altri paesi. Oltre a ciò, esso è ingegnerizzato in modo tale da risultare separata la funzionalità normativa dalle altre numerose funzionalità organizzative e di controllo operativo ed economico della gestione, quindi, il problema dell'adattabilità normativa è facilmente superabile anche nel caso in cui le differenze, tra il sistema italiano ed il sistema di qualunque altro paese, risultino sostanziali. Di fatto Progetto Win Sm@.R.T.® è installato anche in altri paesi della Comunità Europea e sta affrontando altri mercati limitrofi.

Le aziende che in Italia si sono rivolte a Progetto Win Sm@.R.T.® ed alle funzionalità da esso offerte sono, per dimensione dei problemi e qualità della gestione, una garanzia di diffusione internazionale del prodotto in quanto si può ritenere che anche in altri paesi l'obiettivo, da parte dei potenziali clienti, di raggiungere

¹ SISTRI: SIStema di Tracciabilità dei Rifiuti, il sistema informatico che il Ministero dell'Ambiente e della Tutela del Territorio e del Mare intendeva adottare per l'identificazione delle movimentazioni sul territorio di rifiuti speciali e pericolosi con l'ulteriore intento di sostituire la documentazione cartacea ancora vigente.

una più agevole certificazione di qualità ambientale della propria produzione, collimi con l'informatizzazione della gestione dei rifiuti per mezzo di Progetto Win Sm@.R.T.®.

Le automazioni raggiunte con l'uso di Progetto Win Sm@.R.T.® nei settori del controllo degli automezzi sul territorio, dell'ottimizzazione dei percorsi, dell'identificazione automatica dei conferimenti ed altro ancora, pone Progetto Win Sm@.R.T.® quale punto di riferimento obbligato per la risoluzione garantita di problemi organizzativi del settore della gestione dei rifiuti industriali ma anche della gestione pubblica della raccolta e dello smaltimento dei rifiuti.

Un ulteriore campo di applicazione della suite di prodotti Progetto Win Sm@.R.T.® è la gestione della TARI (Tariffa Rifiuti), ovvero, la modalità che, in base alle evoluzioni normative di applicazione del costo della nettezza urbana ai cittadini, ha sostituito la TARSU (Tassa Asporto Rifiuti Solidi Urbani) su tutto il territorio nazionale. Le modalità del passaggio da tassa a tariffa è rimasto discrezionale e lasciate alla capacità decisionale degli enti responsabili del territorio: i Comuni o loro organi delegati a tale gestione.

Per un eventuale approfondimento della conoscenza dei prodotti sono disponibili a richiesta e sul sito WEB www.csgroup.it gli allegati tecnici dei prodotti e dei percorsi conoscitivi guidati resi disponibili su supporti multimediali.

I SERVIZI

La gamma di servizi offerti da Computer Solutions® S.p.A. può essere suddivisa in due tipologie differenti. Da un lato si può collocare l'insieme dei servizi strettamente connessi alla vendita del prodotto Progetto Win Sm@.R.T.®:

- system integration con ambienti software preesistenti² e con sistemi di rilevazione di grandezze analogico digitali³
- assistenza post-vendita
- help-desk sui prodotti
- manutenzione e aggiornamento dell'intera gamma
- personalizzazioni e customizzazioni
- hot-line

Dall'altro invece si possono includere quei servizi collegati soltanto indirettamente con il core business dell'azienda, che vengono erogati da Computer Solutions® S.p.A. grazie alla notevole esperienza maturata nel campo della produzione di software applicativo intimamente legato alla gestione amministrativa dello smaltimento e del recupero dei rifiuti:

- consulenza normativa e controllo Qualità Ambientale
- consulenza nell'identificazione dei modelli organizzativi dedicati alla prevenzione di incidenti con conseguenze ambientali
- formazione
- trasferimento continuativo di know how con l'attività di Academy

² Sistemi ERP ospiti, sistemi di Datawarehouse, sistemi di controllo della produzione, sistemi di work flow management, sistemi di document management, sistemi di rilevazione presenze, etc.

³ Sistemi di rilevazione del peso, sistemi di rilevazione dei flussi di materiale allo stato liquido, sistemi di rilevazione di parametri chimico fisici, sistemi di controllo accessi, sistemi di rilevazione automatica delle targhe automezzi, etc.

LA SOCIETÀ SUL TERRITORIO

La Società ha le seguenti sedi:

FILIALE DI VENEZIA e Uffici Amministrativi

Via Toffoli, 21
30175 VENEZIA MARGHERA
Tel. 041 2582001
Fax 041 2582017
email: mail@csgroup.it
Referente: Dr. E. Agostini

FILIALE DI MONZA

Via Iseo, 13/A
20900 MONZA MB
Tel. 039 747591
Fax 039 2727605
email: mail@csgroup.it
Referente: Ing. A. Ruisi

FILIALE DI ROMA e Sede Legale

Via L. Gaurico, 9/11
00143 ROMA
Tel. 06 59606565
Fax 06 59633658
email: mail@csgroup.it
Referente: Sig. F. Riccioni

FILIALE DI VIAREGGIO LU

Via A. Vespucci, 289
55049 VIAREGGIO LU
Tel. 05841783553
Fax 05831770198
email: mail@csgroup.it
Referente: Dr. A. Cima

FILIALE DI CROTONE

Via Immacolata, 10
88817 CARFIZZI KR
Tel. 0962 87330
Fax 0962 87333
email: mail@csgroup.it
Referente: Dr.ssa G. Affatato

(omissis)

CERTIFICAZIONE DI QUALITA'

Da marzo 2004 Computer Solutions® S.p.A. è certificata in qualità e da marzo 2017 la certificazione è conforme alla norma ISO 9001:2015 nei processi aziendali inerenti:

- **progettazione, studio e sviluppo di software in campo ambientale;**
- **servizi di installazione, avviamento, formazione, bollettazione ed assistenza collegati al software gestito;**
- **formazione e consulenza nel settore della gestione dei rifiuti.**



(omissis)

INDIVIDUAZIONE DELLE ATTIVITÀ A RISCHIO DI COMMISSIONE DI REATI

INDIVIDUAZIONE DELLE AREE E DEI FATTORI DI RISCHIO

In relazione alle attività svolte da Computer Solutions S.p.A., a seguito di specifica analisi dei rischi, anche in considerazione di quanto indicato dal documento di Analisi Rischi e Opportunità dei Processi Aziendali, redatto nell'ambito delle procedure di qualità conformi alla certificazione ISO 9001:2015, sono individuate le seguenti aree o settori funzionali nel cui ambito si possono manifestare fattori di rischio relativi alla commissione di violazioni delle norme penali indicate dal D.Lgs. n. 231 del 2001 o, in generale, del Codice Etico.

AREA	FATTORI DI RISCHIO	PROCESSI
AREA 1 appalti pubblici	nella partecipazione a pubbliche gare o trattative per l'affidamento di lavori pubblici in appalto o in concessione, fattori di rischio relativi alle fasi delle procedure selettive, di autorizzazione del subappalto, di gestione dell'eventuale contenzioso con il committente	P2 P4 P5
AREA 2 attività caratteristica	fattori di rischio relativi a comportamenti che costituiscono violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	P2 P6 P8 P9
	fattori di rischio relativi alle attività di selezione e gestione del personale	
	fattori di rischio relativi alle attività gestione dei sistemi informativi	
AREA 3 servizi gestionali	fattori di rischio relativi alle attività finanziarie, amministrative, patrimoniali	P1 P3 P4 P5
AREA 4 rapporti con la Pubblica Amministrazione	fattori di rischio relativi alle attività che implicano un rapporto diretto con pubblici uffici, organi ispettivi, enti pubblici erogatori di contributi o titolari di poteri autorizzativi, concessori od abilitativi	P2 P3 P5 P7 P8
AREA 5 Comunicazioni sociali e controlli	fattori di rischio relativi alla scorretta o incompleta rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci e nei documenti ad uso informativo, sia interno che	P1 P3 P4 P5 P7 P8
	fattori di rischio relativi a comportamenti idonei ad ostacolare da parte dei soggetti e delle autorità competenti i controlli preventivi sulla attività e sulla rappresentazione contabile dell'attività d'impresa	
AREA 6 rapporti con soci, creditori e terzi	fattori di rischio di comportamenti anche solo potenzialmente pregiudizievoli dell'interesse dei soci, dei creditori e dei terzi.	P3 P4 P7
	in caso di situazioni di conflitto di interessi, fattori di rischio relativi alla attuazione di operazioni di gestione o organizzative interne a condizioni svantaggiose per la Società od alla omissione di decisioni vantag-	

PROCESSI SENSIBILI RELATIVI ALLE AREE A RISCHIO

Sono individuati i seguenti processi sensibili, comuni allo svolgimento delle attività di Computer Solutions S.p.A. relativi alle aree o settori funzionali precedentemente descritti:

#	PROCESSI	REATI
P1	Processi di gestione economico-finanziaria <ul style="list-style-type: none"> - Richiesta d'acquisto - Richiesta d'offerta - Emissione dell'ordine d'acquisto - Ricevimento e controllo della fattura passiva e contabilizzazione - Pagamento e contabilizzazione 	Truffa aggravata ai danni dello Stato; Reati in tema di erogazioni pubbliche; Reati societari
P2	Processo commerciale e partecipazione a gare d'appalto <ul style="list-style-type: none"> - Partecipazione a gare ed appalti pubblici - Risposte a richieste d'offerta private e predisposizione di offerte - Definizione del prezzo o del ribasso - Esecuzione lavori: responsabile di commessa e predisposizione commessa su supporto informatico - Emissione e trasmissione SAL e verbali di consegna - Fatturazione attiva e contabilizzazione - Incasso e contabilizzazione 	Corruzione e concussione; Truffa aggravata ai danni dello Stato; Delitti con finalità di terrorismo
P3	Processo per lo svolgimento di attività come investimento anche per attività di R&S <ul style="list-style-type: none"> - Valutazione dell'opportunità dell'operazione - Nomina del Responsabile di commessa - Predisposizione del dossier di commessa - Rendicontazione di commessa in progetti finanziati con contributo Pubblico - Svolgimento e rendicontazione di commessa 	Corruzione e concussione Truffa aggravata ai danni dello Stato; Reati in tema di erogazioni pubbliche; Reati societari
P4	Processo finanziario <ul style="list-style-type: none"> - Apertura, utilizzo, controllo e chiusura dei conti correnti - Scadenziario pagamenti - Coordinate bancarie dei fornitori - Operazioni di verifica dei pagamenti - Scadenziario incassi - Operazioni di verifica degli incassi - Riconciliazioni bancarie - Finanziamenti 	Reati societari; Delitti con finalità di terrorismo; Riciclaggio.
P5	Processo amministrativo <ul style="list-style-type: none"> - Definizione delle deleghe e dei poteri - Strumenti contabili ed organizzazione del piano dei conti - Contabilizzazione ed archiviazione - Redazione del bilancio - Poste valutative del bilancio 	Reati societari; Riciclaggio.
P6	Processo di gestione dei sistemi informativi, anche di terzi <ul style="list-style-type: none"> - Definizione della funzione responsabile dei sistemi informativi - Protezione fisica dei dati - Utilizzo dei sistemi informativi - Corretto utilizzo di prodotti software di proprietà della Società e di proprietà di terze parti - Attività sui sistemi informativi di terzi 	Frode informatica ai danni dello Stato; Delitti informatici e trattamento illecito di dati; Delitti in materia di violazione del diritto d'autore; Reati ambientali inerenti la gestione dei dati; Detenzione di materiale pedo/pornografico.

p7	Processi di gestione economico legale - Gestione delle comunicazioni ai soci, riguardo alla situazione economica, patrimoniale e finanziaria della Società - Gestione dei rapporti con il Collegio Sindacale e con i Soci	Reati societari; False comunicazioni sociali
p8	Processi di gestione delle risorse umane - Selezione del personale - Costituzione del rapporto di lavoro - assunzioni - Pagamento delle retribuzioni, dei premi e dei rimborsi - Diffusione delle politiche del personale - Valorizzazione e formazione del personale - Informazione e formazione per l'applicazione del Modello - Gestione del tempo di lavoro dei collaboratori - Salute e sicurezza - Gestione delle informazioni e privacy - Integrità e tutela della persona - Protezione del segreto aziendale - Conflitti di interesse - Utilizzo e salvaguardia dei beni di proprietà dell'Azienda - Regali, omaggi e benefici - Rispetto delle norme contenute nel Codice Etico - Molestie o mobbing sul luogo di lavoro - Abuso di sostanze alcoliche o stupefacenti e divieto di fumo	Delitti contro la personalità individuale; Riduzione o mantenimento in schiavitù o in servitù; Reati in tema di erogazioni pubbliche; Reati societari
p9	Processi di gestione della sicurezza - Individuazione dei responsabili - Documento di Valutazione dei Rischi - Sistema di controllo	Danni gravi alla persona; Omicidio colposo

Il Modello Organizzativo, nella Parte Speciale, prescrive, per ciascun processo sensibile individuato, le modalità di svolgimento delle relative attività ed indica, ove rilevanti, le specifiche procedure cui attenersi.

MODELLO ORGANIZZATIVO DI GESTIONE E CONTROLLO: PARTE SPECIALE

PROCESSO DI ATTUAZIONE DEL MODELLO

PROCESSO DI ADOZIONE E ATTUAZIONE DEL MOG

Deve essere definito con data certa che il Modello Organizzativo di Gestione e Controllo è stato adottato, è stato reso operativo e sia idoneo a prevenire i reati.

Le fasi (registrabili) dell'attivazione del MOG sono:

- a) fase di approvazione (verbalizzata) da parte del CdA.
- b) fase di divulgazione (affissione in bacheca, riunioni generali del personale, attività di formazione pertinenti, intranet aziendale)
- c) fase di nomina dell'Organismo di Vigilanza terzo e indipendente, che deve essere dotato cioè di autonomi poteri di iniziativa e di controllo
- d) fase di realizzazione di attività di audizioni e ispezioni.

La giurisprudenza afferma che la circostanza della nomina di un organismo di vigilanza "dotato di autonomi poteri di iniziativa e di controllo", nel periodo precedente al dibattimento, sia il prerequisite necessario per l'accertamento dell'operatività e dell'efficacia del MOG.

(omissis)

ORGANISMO DI VIGILANZA

Gli artt. 6 e 7 del Decreto prevedono che l'ente possa essere esonerato dalla responsabilità connessa alla commissione dei reati indicati nel Decreto qualora l'organo dirigente abbia, fra l'altro:

- a) adottato il modello di organizzazione, gestione e controllo e lo abbia efficacemente attuato, e
- b) affidato il compito di vigilare sul funzionamento e sull'osservanza del modello di organizzazione, gestione e controllo e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

Computer Solutions S.p.A. ha istituito l'Organismo di vigilanza e ha determinato i suoi poteri, responsabilità e compiti più oltre specificati. La responsabilità degli aggiornamenti ed adeguamenti del Modello Organizzativo, nonostante l'istituzione dell'Organismo di vigilanza, è rimessa direttamente al Consiglio di Amministrazione di Computer Solutions S.p.A., sentite le considerazioni e le proposte dell'Organismo di vigilanza. A riguardo, si precisa che il Consiglio di Amministrazione, pur con l'istituzione dell'Organismo di vigilanza, mantiene invariate tutte le attribuzioni e le responsabilità previste dalla legge, dal citato Decreto e dal codice civile in generale, alle quali si aggiunge quella relativa all'adozione, al rispetto delle disposizioni e all'efficacia del Modello Organizzativo, nonché all'istituzione dell'Organismo di vigilanza. Nel contempo, le attività necessarie e strumentali all'attuazione delle disposizioni del Modello Organizzativo sono poste in essere direttamente dalle Funzioni aziendali, sotto la responsabilità del Responsabile di ogni Unità Organizzativa, del Responsabile di ogni Funzione aziendale e del Responsabile di ogni Area aziendale.

REQUISITI DELL'ORGANISMO DI VIGILANZA

L'Organismo di vigilanza di Computer Solutions S.p.A.:

- è dotato di requisiti di indipendenza e autonomia;
- possiede adeguata professionalità;
- è dotato di autonomi poteri di iniziativa e controllo;
- possiede il requisito della continuità di azione.

INDIPENDENZA ED AUTONOMIA

La necessaria autonomia dei membri dell'Organismo di vigilanza di Computer Solutions S.p.a. è garantita in ragione della:

- collocazione in posizione gerarchica di vertice in Computer Solutions S.p.a. assicurata dal riporto in modo diretto ed esclusivo al Consiglio di Amministrazione;
- emanazione in autonomia di un proprio Regolamento messo a conoscenza del Consiglio di Amministrazione;
- dotazione di adeguate risorse finanziarie che vengono utilizzate per ogni esigenza necessaria al corretto svolgimento delle attività proprie dell'Organismo di vigilanza. Del fondo avuto in dotazione

L'Organismo di vigilanza dovrà rendere conto con cadenza annuale al Consiglio di Amministrazione chiedendo, se del caso, opportune integrazioni dello stesso;

- assenza di soggezione, in forza di tale qualità e nell'ambito di svolgimento della propria funzione, al potere gerarchico e disciplinare di alcun altro organo o funzione societaria;
- assenza di incarichi operativi nella Società;
- assenza di conflitti di interessi e di legami di parentela con i vertici della Società;
- presenza dei requisiti di onorabilità di cui alle disposizioni in tema di cause di ineleggibilità e decadenza previste per l'elezione alla carica di sindaco nelle società per azioni di cui all'art. 2399, 1° comma del codice civile.

PROFESSIONALITÀ

L'Organismo di vigilanza è composto da professionisti esterni dotati di specifiche competenze tecniche nel campo delle eventuali e autonome procedure di controllo interno, della valutazione dei rischi e delle misure per il loro contenimento, nonché da esperti di materie giuridiche rilevanti ai fini del Decreto. L'Organismo di vigilanza, nello svolgimento della propria attività, inoltre:

- si avvale del supporto delle Aree aziendali e delle Funzioni aziendali della Società;
- si può avvalere di risorse esterne a Computer Solutions S.p.a. (es.: servizi professionali e/o di consulenza specialistica).

AUTONOMIA NEI POTERI DI INIZIATIVA E CONTROLLO

L'Organismo di vigilanza di Computer Solutions S.p.a. definisce e svolge in modo autonomo le attività di competenza, comprese le attività precipue di controllo. Le regole di funzionamento interno dell'Organismo di vigilanza sono definite dallo stesso nel proprio Regolamento. Come indicato dalle Linee Guida di Confindustria infatti, mentre il Modello Organizzativo (e sue eventuali modifiche) viene approvato dal Consiglio di Amministrazione, il Regolamento rappresenta l'autoregolamentazione operativa dell'Organismo di vigilanza che, appunto, è approvato in piena autonomia dall'Organismo di vigilanza stesso.

CONTINUITÀ DI AZIONE

I membri dell'Organismo di vigilanza garantiscono un impegno costante nell'attività di vigilanza del Modello Organizzativo. Essi, pur essendo soggetti esterni alla Società, sono a conoscenza della struttura e dell'attività di Computer Solutions S.p.a.. La continuità d'azione è garantita anche dalla predisposizione di canali di raccordo con la Società. L'Organismo di vigilanza infatti è coadiuvato e supportato attivamente dai Responsabili delle Aree aziendali, Responsabili di Funzione e dai Responsabili delle Unità Organizzative.

ACQUISIZIONE DELLE INFORMAZIONI

L'acquisizione delle informazioni necessarie all'operatività dell'Organismo di vigilanza viene assicurata, tra l'altro,

- attraverso i flussi informativi verso l'Organismo di vigilanza definiti dal Regolamento e dalla specifico documento *Policy sui flussi di comunicazione con l'Organismo di Vigilanza e dal Modello Organizzativo stesso*;
- attraverso le richieste dell'Organismo di vigilanza stesso verso le strutture interessate;

- attraverso le interviste programmate al personale interno e le verifiche documentali;
- attraverso la partecipazione di uno dei membri dell'Organismo di vigilanza ai momenti decisionali aziendali, laddove vengano trattati temi inerenti i rischi di reato di cui al Decreto.

RIPORTO AGLI ORGANI SOCIALI

L'Organismo di vigilanza riporta direttamente al Consiglio di Amministrazione.

NOMINA DEI MEMBRI DELL'ORGANISMO DI VIGILANZA

Computer Solutions S.p.a. deve costituire l'Organismo di vigilanza deputato alla vigilanza e al controllo del presente Modello Organizzativo. I membri dell'Organismo di vigilanza devono essere nominati tra soggetti esterni a Computer Solutions S.p.a. e devono avere i requisiti indicati dal Decreto e dalle disposizioni in tema di cause di ineleggibilità e decadenza previste per l'elezione alla carica di sindaco nelle società per azioni di cui all'art. 2399, 1° comma del codice civile. L'Organismo di vigilanza rimarrà in carica 3 anni e alla naturale scadenza potrà essere consensualmente riconfermato. Oltre a quanto esplicitato nei paragrafi precedenti, la nomina a membro dell'Organismo di vigilanza comporta:

1. che ciascun membro dell'Organismo di vigilanza è tenuto al rispetto di quanto indicato nel Modello Organizzativo in vigore presso Computer Solutions S.p.a. dal momento della nomina e per tutta la durata del mandato;
2. che ciascun membro dell'Organismo di vigilanza è tenuto al segreto riguardo notizie e informazioni acquisite nell'esercizio delle proprie funzioni. I membri dell'Organismo di vigilanza assicurano la riservatezza delle informazioni acquisite, in particolare, se relative a presunte violazioni del Modello Organizzativo; inoltre, si astengono dal ricercare ed utilizzare informazioni riservate per scopi diversi da quelli previsti dal Decreto, o in ogni caso per fini non conformi ai loro compiti.

Gli obblighi dell'Organismo di vigilanza sono correlati al Modello Organizzativo in vigore durante il periodo di nomina.

RINUNCIA, REVOCA E SANZIONI

Ciascuno dei membri dell'Organismo di vigilanza può rinunciare all'incarico motivando la propria decisione.

Nel pieno rispetto dei principi etici e comportamentali che infondono il Modello Organizzativo, è altresì fatto obbligo a ciascuno dei membri dell'Organismo di vigilanza di presentare le dimissioni dall'incarico nel caso in cui, a qualunque titolo, sopraggiungano cause di incompatibilità e/o di impossibilità per l'effettuazione delle attività e l'assunzione delle proprie responsabilità e/o, comunque, in caso di conflitto di interessi. Il Consiglio di Amministrazione può deliberare la revoca dell'incarico all'OdV soltanto per giustificati motivi. A tale riguardo, per giustificati motivi dovranno intendersi:

- l'interdizione o l'inabilitazione, ovvero una grave infermità che renda uno dei componenti dell'Organismo di vigilanza inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti l'assenza per un periodo superiore a sei mesi;
- un grave inadempimento dei propri doveri così come definiti nel Modello Organizzativo;
- una sentenza di condanna passata in giudicato, a carico di uno dei membri dell'Organismo di vigilanza per aver personalmente commesso uno dei reati previsti dal Decreto;

- una sentenza di condanna passata in giudicato, a carico di uno dei componenti dell'Organismo di vigilanza ad una pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
- l'assenza ingiustificata di un componente dell'Organismo di vigilanza a tre riunioni nell'anno, anche non consecutive, e la mancata collaborazione ai programmi dell'Organismo di vigilanza.

L'Organismo di vigilanza stesso può chiedere al Consiglio di Amministrazione la revoca di uno dei suoi membri per fondati motivi o per evidente conflitto di interesse. Ogni variazione nel tempo della composizione dell'Organismo di vigilanza e la conseguente approvazione delle modifiche al Modello Organizzativo, deve essere deliberata dal Consiglio di Amministrazione, sentito il parere non vincolante dell'Organismo di vigilanza stesso. Tale parere deve essere riportato nel verbale della relativa riunione del Consiglio di Amministrazione.

FUNZIONI, ATTIVITÀ E POTERI DELL'ORGANISMO DI VIGILANZA

L'Organismo di vigilanza è dotato dell'autorità e dei poteri per vigilare in autonomia sul funzionamento e sull'osservanza del Modello Organizzativo, per garantire l'effettività e la razionalità del Modello Organizzativo, per vagliare l'adeguatezza del medesimo. Di seguito, un'elencazione delle funzioni, poteri ed attività attribuite all'Organismo di vigilanza anche sulla base delle indicazioni contenute negli artt. 6 e 7 del Decreto. L'Organismo di vigilanza:

- vigila periodicamente sull'effettività del Modello Organizzativo, che si sostanzia nella verifica della coerenza tra i comportamenti concretamente attuati in azienda e quanto previsto dalle disposizioni contenute nel Modello Organizzativo;
- valuta l'adeguatezza del Modello Organizzativo: ossia della sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;
- analizza periodicamente il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello Organizzativo;
- conduce ricognizioni dell'attività aziendale ai fini dell'aggiornamento della mappatura delle aree a rischio-reato;
- cura l'aggiornamento necessario del Modello Organizzativo nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni ed adeguamenti. Tale aggiornamento si divide in due fasi distinte ed integrate:
 - o presentazione di proposte di adeguamento del Modello Organizzativo verso il Consiglio di Amministrazione. A seconda della tipologia e della portata degli interventi, le proposte di adeguamento potranno essere dirette anche verso le specifiche Funzioni aziendali;
 - o *follow-up*, ovvero verifica sistematica e compiuta dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte e definite.
- gestisce, approfondisce e verifica la normativa oggetto del Codice Etico al fine di adeguarlo all'evoluzione legislativa e dei contratti collettivi;
- promuove le iniziative per la diffusione della conoscenza del Modello Organizzativo, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello Organizzativo, di concerto con il CEO;
- ha la facoltà di chiedere e/o assegnare a soggetti terzi, in possesso delle competenze specifiche necessarie per la migliore esecuzione dell'incarico, compiti di natura meramente tecnica;
- può procedere ad interventi di controllo in qualsiasi momento, nell'ambito della propria autonomia e discrezionalità;
- può accedere senza limitazioni alle informazioni aziendali per svolgere le attività allo stesso delegate;

- può consultare documenti, accedere ai sistemi informativi aziendali per acquisire dati e/o informazioni necessari alle attività di analisi, verificare l'operato delle funzioni nonché effettuare interviste alle persone preposte nelle singole fasi di un determinato processo a rischio;
- effettua controlli sul comportamento degli utenti degli strumenti informatici avvalendosi della collaborazione della funzione della Direzione Tecnica, a cui l'Organismo di vigilanza periodicamente chiederà informazioni riguardo la sussistenza o meno di eventuali problematiche nell'utilizzazione degli strumenti informatici da parte degli utenti. Le verifiche compiute dall'Organismo di vigilanza saranno condotte sempre nel rispetto del diritto di riservatezza degli utenti e dei titolari dei dati trattati, anche rispetto ai rapporti esterni tenuti attraverso gli strumenti informatici;
- partecipa per mezzo di un proprio membro, alle riunioni del Consiglio di amministrazione o qualsiasi altro comitato, qualora vengano trattati temi inerenti i rischi di reato ai sensi del Decreto;
- valuta i risultati delle verifiche effettuate o delle informazioni ricevute ed il loro impatto sul Modello Organizzativo.

Lo svolgimento delle attività sopra indicate è affiancata e coadiuvata:

- dal rispetto da parte dei Soggetti Destinatari delle regole sui flussi informativi verso l'Organismo di vigilanza nonché dell'obbligo di dare riscontro a specifiche richieste informative formulate dall'OdV, come previsto dal Modello Organizzativo;
- dal rispetto da parte dell'OdV dell'obbligo di riporto scritto e orale verso il Consiglio di Amministrazione, nonché dell'obbligo di dare riscontro a specifiche richieste informative del Consiglio di Amministrazione come previsto dal Modello Organizzativo.

In caso di violazioni direttamente riscontrate o segnalate l'OdV:

- verifica, controlla e valuta i casi di violazione delle norme aziendali, provvedendo, nel caso di infrazioni, alle misure opportune, in collaborazione con i responsabili aziendali competenti nel rispetto delle leggi, dei regolamenti e dei contratti collettivi;
- conduce approfondimenti per l'accertamento di presunte violazioni delle prescrizioni del presente Modello Organizzativo;
- segnala, al Consiglio di Amministrazione, al Collegio Sindacale e al CEO la notizia di violazione del Modello Organizzativo;
- monitora, di concerto con il Consiglio di Amministrazione e con il CEO, l'applicazione delle sanzioni disciplinari;
- tutela i soggetti che segnalano comportamenti non conformi al Codice Etico e alle disposizioni di cui al Modello Organizzativo, attraverso iniziative concordate con il CEO.

Ai fini della gestione e prevenzione del rischio di violazioni attinenti la normativa di salute e sicurezza sul lavoro, l'Organismo di vigilanza esegue un controllo dell'efficienza ed efficacia delle procedure rilevanti ai sensi del Decreto del tutto indipendente e differenziata dall'attività di controllo tecnico-operativa di competenza del RSPP.

(omissis)



CODICE ETICO

Sommario

PREMESSA.....	3
DISPOSIZIONI GENERALI	3
AMBITO DI APPLICAZIONE E DESTINATARI	3
PRINCIPI GENERALI.....	4
COMUNICAZIONE	4
RESPONSABILITÀ.....	4
CORRETTEZZA	4
CONFLITTO DI INTERESSE.....	5
RISERVATEZZA.....	5
COMPORAMENTO NEGLI AFFARI.....	5
RELAZIONI D’AFFARI	5
TUTELA DELLA CONCORRENZA	5
RAPPORTI CON I FORNITORI	6
RAPPORTI CON LE ISTITUZIONI.....	6
SALUTE, SICUREZZA E AMBIENTE.....	6
SALUTE, SICUREZZA, AMBIENTE	6
SISTEMA SANZIONATORIO	6
SISTEMA SANZIONATORIO	6
PROVVEDIMENTI SANZIONATORI	7
DISPOSIZIONI FINALI.....	7
DISPOSIZIONI FINALI	7

PREMESSA

La Computer Solutions S.p.A. è di sicuro tra le principali aziende produttrici di software dedicato alla soluzione delle problematiche legate alla gestione normativa ed amministrativa dei rifiuti. In tutte le fasi della sua crescita la Computer Solutions® S.p.A. ha perseguito l'obiettivo di svolgere le proprie attività nel rispetto delle leggi e i dei regolamenti vigenti sia in Italia che in tutti i paesi in cui ha operato con contatti operativi e commerciali. A tal fine la Computer Solutions® S.p.A. favorisce un ambiente di lavoro che, ispirato al rispetto, alla correttezza ed alla collaborazione, permette il coinvolgimento e la responsabilizzazione di dipendenti e collaboratori, con riguardo agli specifici obiettivi da raggiungere e alle modalità per perseguirli. La Computer Solutions® S.p.A. agisce in ottemperanza dei principi di lealtà, correttezza, responsabilità, libertà, dignità della persona umana e rispetto delle diversità e ripudia ogni discriminazione basata sul sesso, sulle razze, sulle lingue, sulle condizioni personali e sociali, sul credo religioso e politico. Nel recente contesto di crescente attenzione verso la gestione aziendale, la Computer Solutions® S.p.A. ispira la propria attività interna ed esterna al rispetto dei principi contenuti nel presente documento (di seguito "Codice Etico"), che rappresenta, tra l'altro, una componente fondante dei modelli di organizzazione, gestione e controllo adottata da Computer Solutions® S.p.A. ai sensi del D.Lgs. 231/01 e del complessivo sistema di controllo interno della Società, nel convincimento che l'etica nella conduzione degli affari sia da perseguire quale condizione del successo dell'impresa. Al fine di raggiungere lo scopo prefissato, si sono tenuti in considerazione i suggerimenti formulati nelle Linee Guida di Confindustria. In questa prospettiva, i principi e i valori espressi nel Codice Etico costituiscono anche un utile riferimento interpretativo nella concreta applicazione del D.Lgs. 231/01 in relazione alle dinamiche aziendali. Il Codice Etico è stato predisposto con l'obiettivo di definire con chiarezza l'insieme dei valori che la Computer Solutions® S.p.A. riconosce, accetta e condivide. La Computer Solutions® S.p.A. assicura un'attività di diffusione ed informazione sulle disposizioni del Codice Etico e sull'applicazione dello stesso ai soggetti cui si riferisce, in modo che i dipendenti, gli amministratori e tutti coloro che operano per la Computer Solutions® S.p.A. svolgano la propria attività e/o il proprio incarico secondo una costante e stretta osservanza dei principi e dei valori in esso contenuti.

DISPOSIZIONI GENERALI

Ambito di applicazione e Destinatari

1. Le disposizioni del presente Codice Etico esprimono i principi fondamentali cui si ispira la Computer Solutions® S.p.A. e costituiscono altresì specificazioni esemplificative degli obblighi generali di diligenza, correttezza e lealtà che qualificano l'adempimento delle prestazioni lavorative e il comportamento nell'ambiente di lavoro.
2. I principi e le disposizioni del Codice Etico sono vincolanti per gli amministratori ("Amministratori") e i sindaci ("Sindaci"), per tutte le persone legate da rapporti di lavoro subordinato con la Computer Solutions® S.p.A. ("Dipendenti") e per tutti coloro che operano per la Computer Solutions® S.p.A., quale che sia il rapporto, anche temporaneo, che li lega alla stessa ("Collaboratori"). Gli Amministratori, i Sindaci, i Dipendenti e i Collaboratori sono di seguito definiti congiuntamente "Destinatari".
3. Il Codice Etico è portato a conoscenza anche di tutti i soggetti terzi che ricevano incarichi dalla Computer Solutions® S.p.A. o che abbiano con essa rapporti stabili o temporanei.

Principi generali

1. Il Codice Etico costituisce un insieme di principi la cui osservanza è di fondamentale importanza per il regolare funzionamento, l'affidabilità della gestione e l'immagine di Computer Solutions® S.p.A.. A tali principi si richiamano le operazioni, i comportamenti e i rapporti, sia interni alla Società sia esterni.
2. La Computer Solutions® S.p.A. riconosce la centralità delle risorse umane e ritiene che un fattore essenziale di successo e di sviluppo dell'impresa sia costituito dal contributo professionale delle persone che vi operano. La gestione delle risorse umane di Computer Solutions S.p.A. è improntata al rispetto della personalità e professionalità di ciascuna di esse, in un quadro di lealtà e fiducia.

Comunicazione

1. La Computer Solutions® S.p.A. provvede ad informare tutti i Destinatari sulle disposizioni e sull'applicazione del Codice Etico, raccomandandone l'osservanza.
2. In particolare, la Computer Solutions® S.p.A., attraverso le funzioni aziendali a ciò preposte, provvede:
 - alla diffusione del Codice Etico presso i Destinatari, mediante la distribuzione di copie dello stesso;
 - all'interpretazione e al chiarimento delle disposizioni contenute nel Codice Etico;
 - alla verifica dell'effettiva osservanza del Codice Etico;
 - agli eventuali futuri aggiornamenti ed implementazione delle disposizioni del Codice Etico, in funzione delle esigenze che di volta in volta si manifestino.
3. Il Codice Etico è altresì pubblicato, con adeguato rilievo, nella sezione "Responsabilità sociale d'impresa" del sito www.csgroup.it.

Responsabilità

Ciascun Destinatario svolge la propria attività lavorativa ed il proprio incarico con impegno professionale, diligenza, efficienza e correttezza, utilizzando al meglio gli strumenti e il tempo a sua disposizione ed assumendo le responsabilità connesse agli impegni relativi.

Correttezza

1. Tutte le azioni e le operazioni compiute ed i comportamenti tenuti da ciascuno dei Destinatari nello svolgimento del proprio incarico o funzione sono ispirati a trasparenza, correttezza e reciproco rispetto nonché alla legittimità sotto l'aspetto sia formale che sostanziale, secondo le norme vigenti e le procedure interne, anche al fine di tutelare il patrimonio e l'immagine aziendale.
2. In particolare, non sono consentiti:
 - il perseguimento di interessi personali o di terzi a discapito di quelli sociali;
 - l'abusivo sfruttamento, nell'interesse personale o di terzi, del nome e della reputazione di Computer Solutions® S.p.A. nonché delle informazioni acquisite e delle opportunità di affari apprese nello svolgimento del proprio incarico o funzione;
 - l'uso di beni e attrezzature di cui i Destinatari dispongano nello svolgimento del proprio incarico o funzione per scopi diversi da quelli ad essi propri.
3. Ciascun Destinatario non accetta, né effettua, per sé o per altri, pressioni, raccomandazioni o segnalazioni, che possano recare pregiudizio a Computer Solutions® S.p.A. o indebiti vantaggi per sé, per la Computer Solutions® S.p.A. o per terzi.

Ciascun Destinatario, altresì, respinge e non effettua promesse e/o offerte indebite di denaro o altri benefici, salvo che questi ultimi siano di modico valore e non correlati a richieste di alcun genere.

4. Qualora il Destinatario riceva da parte di un terzo un' offerta o una richiesta di benefici, salvo omaggi di uso commerciale o di modico valore, ne informa immediatamente il proprio superiore gerarchico o, eventualmente, il soggetto cui sia tenuto, a seconda dei casi, a riferire per le iniziative del caso.

Conflitto di interesse

1. I Destinatari perseguono, nello svolgimento del proprio incarico o funzione, gli obiettivi e gli interessi generali di Computer Solutions® S.p.A. e si astengono, pertanto, da attività, comportamenti e atti comunque incompatibili con gli obblighi connessi al rapporto intrattenuto con Computer Solutions® S.p.A.

2. I Destinatari informano senza ritardo, tenuto conto delle circostanze, il proprio superiore gerarchico o, eventualmente, il soggetto cui siano tenuti, a seconda dei casi, a riferire delle situazioni o attività nelle quali potrebbero essere titolari di interessi in conflitto con quelli di Computer Solutions® S.p.A. (o qualora di tali interessi siano titolari prossimi congiunti) ed in ogni altro caso in cui ricorrano rilevanti ragioni di convenienza. I Destinatari rispettano le decisioni che in proposito sono assunte da Computer Solutions® S.p.A.

Riservatezza

I Destinatari assicurano la massima riservatezza sulle notizie e informazioni costituenti il patrimonio aziendale o inerenti all'attività di Computer Solutions® S.p.A., acquisite e/o elaborate in occasione dell'espletamento del proprio incarico o funzione. Il trattamento delle informazioni riservate è disciplinato - in coerenza con le disposizioni di legge ed i regolamenti applicabili - da apposite procedure interne.

COMPORTAMENTO NEGLI AFFARI

Relazioni d'affari

1. La Computer Solutions S.p.A. nello svolgimento delle relazioni d'affari si ispira ai principi di legalità, lealtà e correttezza.

2. Veridicità, accuratezza, completezza e chiarezza delle informazioni nella registrazione contabile rappresentano valori fondamentali per la Computer Solutions® S.p.A., anche al fine di garantire ai soci e ai terzi la possibilità di avere un'immagine chiara della situazione economica, patrimoniale e finanziaria dell'impresa.

Tutela della Concorrenza

La Computer Solutions® S.p.A. riconosce che una concorrenza corretta, libera e leale costituisce un fattore decisivo di crescita e di costante miglioramento dell'impresa.

Rapporti con i fornitori

La selezione dei fornitori e la determinazione degli acquisti di beni e/o servizi devono avvenire nel rispetto dei principi del presente Codice Etico e sono basate sul servizio nonché sulle garanzie di assistenza, tempestività ed efficienza.

Rapporti con le istituzioni

1. I rapporti di Computer Solutions S.p.A. nei confronti delle istituzioni pubbliche nazionali, comunitarie e internazionali ("Istituzioni") nonché nei confronti di pubblici ufficiali o incaricati di pubblico servizio ovvero organi, rappresentanti, mandatari, esponenti, membri, dipendenti, consulenti, incaricati di pubbliche funzioni o servizi, di pubbliche istituzioni, di pubbliche amministrazioni, di enti pubblici, anche economici, di enti o società pubbliche di carattere locale, nazionale o internazionale ("Pubblici Funzionari") sono intrattenuti da ciascun Amministratore e da ciascun Dipendente, quale che sia la funzione o l'incarico, o, se del caso, da ciascun Collaboratore, nel rispetto della normativa vigente, dei principi definiti nel presente Codice Etico nonché delle procedure aziendali, sulla base dei criteri generali di correttezza e di lealtà.

2. La Computer Solutions® S.p.A., qualora lo ritenga opportuno, può sostenere programmi di enti pubblici intesi a realizzare utilità e benefici per la collettività nonché le attività di fondazioni e associazioni, sempre nel rispetto della normativa vigente, dei principi definiti nel presente Codice Etico e delle procedure aziendali.

SALUTE, SICUREZZA E AMBIENTE

Salute, sicurezza, ambiente

Nell'ambito della propria attività la Computer Solutions® S.p.A. si ispira al principio di rispetto e salvaguardia dell'ambiente e persegue l'obiettivo di tutelare la sicurezza e la salute dei Destinatari, adottando tutte le misure previste a tal fine dalla legge.

1. Adotta le misure più opportune per evitare rischi nello svolgimento delle attività anche con valutazioni periodiche dei rischi stessi.
2. Impartisce adeguata formazione ai Destinatari.

SISTEMA SANZIONATORIO

Sistema sanzionatorio

La violazione delle disposizioni contenute nel presente Codice Etico e nei Modelli 231 (e nelle procedure aziendali ad essi riferibili) comporta, a carico dei Destinatari responsabili di tali violazioni - laddove ritenuto necessario per la tutela degli interessi aziendali e compatibilmente con quanto previsto dal quadro norma-

tivo vigente - l'applicazione dei provvedimenti sanzionatori indicati nei Modelli 231 qui di seguito indicati.

Provvedimenti sanzionatori

Con riferimento a quanto indicato nel capoverso "Sistema sanzionatorio" del Codice Etico, i provvedimenti sanzionatori applicabili ai Destinatari sono i seguenti.

- Per quanto riguarda i Dipendenti, l'osservanza delle norme del Codice Etico e del D.Lgs. 231/01 deve considerarsi parte essenziale delle obbligazioni contrattuali dagli stessi assunte ai sensi e per gli effetti dell'articolo 2104 del Codice Civile; pertanto, i comportamenti da essi tenuti in violazione delle regole comportamentali previste nel Codice Etico e nel D.Lgs. 231/01 sono considerati inadempimento delle obbligazioni primarie del rapporto di lavoro e hanno rilevanza anche quali illeciti disciplinari, nel rispetto delle norme specialistiche (in particolare, CCNL e Contratti Integrativi Aziendali applicabili) e delle procedure di settore vigenti (art. 7 dello Statuto dei Lavoratori).

Il tipo e l'entità delle sanzioni previste dalle previsioni contrattuali vigenti saranno applicate tenendo conto:

- dell'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia evidenziata;
- del comportamento complessivo del Dipendente, con particolare riguardo alla sussistenza o meno di precedenti sanzioni disciplinari;
- della posizione funzionale e alle mansioni del Dipendente coinvolto;
- di altre particolari circostanze rilevanti che accompagnano la violazione.

- Per quanto riguarda i Collaboratori e/o i soggetti aventi relazioni d'affari con Computer Solutions® S.p.A., quale che sia il rapporto, anche temporaneo, che li lega alle stesse, l'inosservanza delle norme del Codice Etico e del D.Lgs. 231/01 potrà, se del caso, costituire inadempimento delle obbligazioni contrattuali assunte, con ogni conseguenza di legge, anche in ordine alla risoluzione del contratto e/o dell'incarico e potrà comportare il risarcimento dei danni subiti dalla società Computer Solutions® S.p.A.

- Con riferimento agli Amministratori e ai Sindaci, gli organi sociali competenti adotteranno di volta in volta le misure di tutela più opportune, nell'ambito di quelle previste dalla normativa vigente.

- Con riferimento ai soggetti costituenti l'Organo di Vigilanza e Controllo di cui al D.Lgs. 231/01, nel caso in cui il rapporto con la società Computer Solutions® S.p.A. sia di lavoro subordinato, si applicheranno le disposizioni riferibili ai Dipendenti, nel caso in cui, invece, il rapporto sia di collaborazione/consulenza, varrà quanto previsto per i Collaboratori.

DISPOSIZIONI FINALI

Disposizioni finali

Il Codice Etico è approvato dal Consiglio di Amministrazione delle società Computer Solutions® S.p.A. Eventuali futuri aggiornamenti, dovuti ad adeguamenti normativi o all'evoluzione della sensibilità civile, saranno approvati dal Consiglio di Amministrazione e diffusi tempestivamente a tutti i Destinatari.