PARTE SPECIALE

M.O.G.C.

ARECHI MULTISERVICE S.P.A.

Con riferimento alle aree di attività, la Arechi Multiservice S.p.A. ha inquadrato alcuni ambiti in cui si ravvisano criticità tali da determinare un controllo aziendale interno. Detto controllo, oltre a garantire il corretto funzionamento delle aree operative, è teso a scongiurare anche il rischio di commissione di reati rilevanti ai sensi del D.Lgs. 231/01.

PROCEDURE ATTINENTI LA GESTIONE DI FLUSSI DANARO PROCEDURE INFORMATIVE CONTABILI INTERNE – COMUNICAZIONI SOCIALI – RELAZIONI CON ORGANISMI DI VIGILANZA NAZIONALI (art. 25/ter D.Lgs 231/01) (art. 25 octies D.Lgs. 231/01).

Attesa la verificabilità dei flussi economici sia in entrata che in uscita, così come esplicitata in sede operativa nella precedente sezione "Gestione", in questa sede basterà segnalare che gli Esponenti Aziendali, L'Amministratore Unico, sono tenuti ad attenersi a quanto previsto dalla già predisposta disciplina aziendale.

Tali figure dovranno attenersi, per i pagamenti, alla seguente:

a) Effettuare ogni singolo pagamento solo in presenza di espresso giustificativo di spesa;

b) Sottoporre ogni singola operazione di pagamento al controllo primario dell'Amministratore Unico, successivamente far vagliare al soggetto responsabile del settore pagamenti l'operazione e, solo in ultimo, effettuare il controllo di ogni singolo passaggio autorizzando il pagamento tramite firma digitale del documento contabile.

Per ciò che concerne gli incassi, gli stessi sono tracciabili attraverso la registrazione delle singole operazioni portate in fatturazione e rivenienti dal regime di Convenzioni sottoscritte da Arechi Multisevice S.p.A. .

Le evidenze contabili, perciò, assumono grande rilevanza, sia nei rapporti interni che in quelli con l'Amministrazione Provinciale di Salerno, risultando nodo fondamentale della gestione societaria.

Si dispone, quindi, a carico degli Esponenti Aziendali, dei Professionisti e dei Partner, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti dell'Arechi multiservice S.p.A., nell'ambito dell'espletamento delle attività considerate a rischio, **di attenersi ai seguenti principi generali di condotta:**

1. astenersi dal porre in essere comportamenti tali da integrare i Reati descritti all'interno dell'art. 25-*ter* del D.Lgs 231/01;

2. astenersi dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle previste al citato articolo, possano potenzialmente diventarlo;

3. utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione di Reati, di qualunque natura.

4. 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 soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria di Arechi Multiservice S.p.A. e del Gruppo nel suo insieme.

In ordine a tale punto, è **fatto divieto di**:

(a) predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria di Arechi Multiservice S.p.A.;

(b) omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria di Arechi Multiservice S.p.A.;

(c) non attenersi ai principi e alle prescrizioni contenute in norme imperative e ai principi di correttezza Contabile;

5. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nell'acquisizione, elaborazione e comunicazione dei dati e delle informazioni necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria di Arechi Multiservice S.p.A. e sull'evoluzione delle relative attività, nonché sugli strumenti finanziari di Arechi Multiservice S.p.A. e relativi diritti.

In ordine a tale punto, **è fatto divieto di**:

(a) alterare o, comunque, riportare in modo non corretto i dati e le informazioni destinati alla stesura di prospetti informativi;

(b) presentare i dati e le informazioni utilizzati in modo tale da fornire una rappresentazione non corretta e veritiera sulla situazione patrimoniale, economica e finanziaria di Arechi Multiservice S.p.A.;

6. 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**:

(a) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;

(b) 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;

(c) acquistare o far acquistare, sottoscrivere o far 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;

d) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;

e) procedere in ogni modo a formazione o aumento fittizi del capitale sociale;

f) 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;

7. assicurare il regolare funzionamento di Arechi Multiservice S.p.A. 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**:

a) 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;

b) porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;

8. astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata

presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato.

In ordine a tale punto, **è fatto divieto di:**

a) pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio suscettibili di determinare riflessi su strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato ed idonei ad alterarne sensibilmente il prezzo.

9. effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità pubbliche di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

In ordine a tale punto, **è fatto divieto di**:

a) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, tutte le comunicazioni, periodiche e non, previste dalla legge e dalla ulteriore normativa di settore, nonché nei confronti degli organi Finanziari e Tributari della P.A.;

b) la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità;

c) esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria di Arechi Multiservice S.p.A. e del Gruppo nel suo insieme;

d) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di Vigilanza, anche in sede di ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Principi procedurali

1. Nelle attività di predisposizione delle comunicazioni indirizzate ai soci, ed al pubblico in generale, contenenti informazioni e dati sulla situazione economica patrimoniale e finanziaria della società – e, in particolare, ai fini della formazione del bilancio, della relazione semestrale, delle relazioni trimestrali e di altre situazioni contabili infrannuali delle Società, nonché del bilancio consolidato – dovrà essere seguito il seguente procedimento:

a) il preposto alla redazione dei documenti contabili societari con l'Amministratore Unico sono tenuti a rilasciare un'apposita relazione con relativa attestazione del Collegio Sindacale e del RPC della società attestante:

a2) la veridicità, correttezza, precisione e completezza dei dati e delle informazioni contenute nel bilancio ovvero negli altri documenti contabili sopra indicati e nei documenti connessi, nonché degli elementi informativi messi a disposizione dalla società stessa;

a3) l'insussistenza di elementi da cui poter desumere che le dichiarazioni e i dati raccolti contengano elementi incompleti o inesatti;

a4) il rispetto di procedure tese a fornire una ragionevole certezza sulla correttezza, precisione e completezza delle informazioni e dei dati contenuti nei documenti sopra indicati;

a5) il rispetto delle procedure previste dal presente paragrafo.

a6) la dichiarazione di cui alla lettera a) deve essere:

• presentata all'Amministratore Unico e/o al Consiglio di Amministrazione in occasione della delibera di approvazione del proprio progetto di bilancio civilistico e del bilancio consolidato;

• trasmessa in copia all'ODV di Arechi Multiservice S.p.A.;

• trasmessa in copia al Dirigente Preposto alla Redazione dei Documenti Contabili della Amministrazione Provinciale di Salerno.

ODV di Arechi Multiservice S.p.A. provvederà al coordinamento del procedimento descritto.

Nelle attività di trattamento, gestione e comunicazione verso l'esterno di notizie o dati riguardanti la Società, è fatto obbligo agli Esponenti Aziendali di attenersi a quanto previsto nelle procedure interne in materia di informazioni riservate o privilegiate.

Nella predisposizione di comunicazioni alle Autorità pubbliche di Vigilanza e gestione dei rapporti con le stesse, occorrerà porre particolare attenzione al rispetto:

a) delle disposizioni di legge e di regolamento concernenti le comunicazioni, periodiche e non, da inviare a tali Autorità;

b) degli obblighi di trasmissione alle Autorità suddette dei dati e documenti previsti dalle norme in vigore ovvero specificamente richiesti dalle predette Autorità;

c) degli obblighi di collaborazione da fornire nel corso di eventuali accertamenti ispettivi.

PROCEDURE INFORMATICHE E TRATTAMENTO DATI.

(Art. 24 bis, D.Lgs. 231/2001)

I dipendenti, i collaboratori, i professionisti esterni e tutti i soggetti rientranti nella definizione di "stakeholders" dovranno attenersi alla disciplina aziendale.

Preliminarmente si segnala che con determina del 21 maggio 2018 l'Amministratore Unico ha deliberato di non doversi procedere alla nomina un Responsabile della Protezione Dati ex Reg. EU n.679/16, tale decisione è stata presa in virtù della non necessarietà di tale figura sia per la quantità che qualità di dati trattati relativamente a persone fisiche.

In via generale, a dipendenti, collaboratori, professionisti esterni e "stakeholders" è richiesto di:

non porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate ex art. 24-bis del d.lgs. 231/2001;

non violare i principi e le procedure aziendali previste;

non porre in essere comportamenti in contrasto con leggi e regolamenti in materia di protezione e sicurezza di dati personali e sistemi informatici (in particolare, Codice in materia di protezione dei dati personali; provvedimenti del Garante della Privacy, Reg. UE 679/16, ecc.).

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

c) accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;

d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;

h) istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i collaboratori e dipendenti indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica;
3. segnalare alle funzioni competenti il furto, il danneggiamento o lo smarrimento di tali strumenti; inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla funzione competente l'originale della denuncia all'Autorità di Pubblica Sicurezza;
4. evitare di introdurre e/o conservare in Società (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;
5. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC;
7. evitare l'utilizzo di passwords di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi;

8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

Il sistema dei controlli, adattato dalla Società prevede, con riferimento alle singole aree a rischio individuate, una serie di protocolli di controllo di seguito descritti e applicabili a tutte le aree a rischio.

− Ogni comunicazione, anche a terzi, deve essere inoltrata tramite sistema e-mail, in tal modo ogni attività inerente le singole pratiche e/o posizioni, potrà essere costantemente monitorata. Per le comunicazioni interne sarà sempre possibile

avvalersi del sistema e-mail ed è fatto divieto eliminare o distruggere i file già inviati, i quali dovranno essere archiviati nelle apposite banche dati;

− L'Amministratore Unico, avrà libero accesso in qualsiasi momento alle banche dati dei singoli dipendenti. Con persona che sarà all'uopo incaricata l'A.U. effettuerà controlli periodici, con cadenza quadrimestrale, sul corretto utilizzo degli applicativi informatici da parte di dipendenti e collaboratori, siano essi interni o esterni;

− I dipendenti e i collaboratori effettueranno l'accesso ai sistemi informatici solo con le proprie credenziali e per le finalità delle mansioni aziendali assegnate. Responsabile per i sistemi informatici nonché per le modalità e la gestione degli accessi è il Dott. Vito L. M. Brindisi, il quale garantirà ai singoli soggetti interessati accessi sicuri ed univoci. Chiunque violi detto protocollo sarà passibile di sanzione disciplinare;

− La Società si impegna, sempre con cadenza quadrimestrale, ad effettuare controlli tesi ad assicurare:

il corretto e sicuro funzionamento degli elaboratori di informazioni;
la protezione da software pericoloso;
il backup di informazioni e software;
la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
il controllo sui cambiamenti agli elaboratori e ai sistemi;

la gestione di dispositivi rimovibili.

− Inoltre la Società, sempre nell'ambito in oggetto e per garantire il corretto funzionamento degli applicativi informatici (software e hardware), si impegna ad effettuare controlli di verifica tramite:

la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

Con riferimento all'attività di gestione dei profili utente e del processo di autenticazione la Società si conforma ai seguenti principi, e nello specifico prevede:

l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;

una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
i piani e le procedure operative per le attività di telelavoro.

Nel caso che vengano rilevate anomalie di sistema, incidenti e problemi circa la sicurezza informatica, il dipendente o il collaboratore che abbia rilevato detto segnale patologico dovrà darne immediata notizia all'A.U. e al responsabile dei sistemi informatici Dott. Vito L. M. Brindisi
Il responsabile dei sistemi informatici, quindi, sarà tenuto a garantire:
appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;
l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;

la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;

l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;

appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;

l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;

l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;

la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;

la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.

Per ciò che concerne l'utilizzo del sistema informatico aziendale a soggetti esterni, lo stesso è precluso a tale categoria di utenti. Sarà sempre cura del responsabile dei sistemi informatici vigilare sulla titolarità dei soggetti che accedono al sistema ed impedire che soggetti estranei alla Società detengano nome utente e password per l'accesso al sistema aziendale.

RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (Artt. 24 e 25 D.lgs 231/01)

La Società si impegna a svolgere la propria attività ponendo in essere comportamenti che non siano in diretto contrasto con quanto previsto dagli artt. 24 e 25 del D.lgs 231/01.

La Società è dotata di un piano anticorruzione che applica alla prassi aziendale, lo stesso specifica, tra l'altro, anche gli obblighi dei soggetti nei rapporti con la Pubblica Amministrazione e tutti gli adempimenti previsti dall'ANAC sono monitorati dal responsabile dell'anticorruzione Dott. Emilio Iannone.

Ciononostante la Arechi Multiservice S.p.A., proprio in virtù della sua peculiare caratteristica di società in-house della Amministrazione Provinciale di Salerno, intende ribadire che la condotta dei soggetti aziendali è sempre improntata a principi di correttezza e buona fede e, quindi, rinnova le linee guida di comportamento.

Più nello specifico è fatto assoluto divieto, nei rapporti con Enti pubblici, e Pubblica Amministrazione in genere, assumere o mettere in atto comportamenti che:

1) nell'esercizio delle attività oggetto delle autorizzazioni/licenze, possano essere finalizzati ad evitare, anche in parte, l'osservanza degli adempimenti di legge/amministrativi o, comunque, a poter disporre di indebiti privilegi;

2) in sede di adempimenti conseguenti agli obblighi di legge/normativi e di attività di gestione in genere, possano essere diretti a rappresentare alla Pubblica Amministrazione dati/informazioni non corretti, con la finalità di perseguire "posizioni privilegiate" nell'interesse della Società o di eludere obblighi di legge/normativi;

3) in sede di ispezioni/controlli/verifiche da parte di Autorità Indipendenti/Organismi di Vigilanza/Ministeri/Rappresentanti delle Istituzioni, possano essere finalizzati a influenzare indebitamente, nell'interesse della Società, il giudizio/parere di tali Organismi;

4) Nell'espletamento delle rispettive attività e funzioni oltre alle regole di cui al presente Modello, gli Esponenti Aziendali sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

• il Codice etico;

• il Regolamento interno per la qualificazione delle imprese da interpellare nelle gare per acquisti, appalti e servizi;

• le procedure operative volte a garantire la trasparenza nel processo di approvvigionamento;

• ogni altra documentazione relativa al sistema di controllo interno in essere in Arechi Multiservice S.p.A.;

• le procedure informative per l'assunzione e la formazione del personale.

Inoltre, si prevede a carico dei Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società nell'ambito dell'espletamento delle attività considerate a rischio, l'espresso divieto di:

a) effettuare elargizioni in denaro a pubblici funzionari italiani o esteri (o a loro familiari, parenti, affini , amici ecc.);

b) distribuire omaggi e regali o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della P.A. (o loro parenti, affini, amici, ecc.), al di fuori di quanto previsto dalla prassi aziendale (vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). Gli omaggi consentiti nell'ambito della Società si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte ad es. non sono di modico valore viaggi e soggiorni, iscrizioni a circoli, ecc.) o la *brand image* della Società medesima. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;

.c) promettere od offrire a rappresentanti della Pubblica Amministrazione (o loro parenti, affini, amici, ecc.) la prestazione di consulenze e/o altri servizi che possano avvantaggiarli a titolo personale;

d) effettuare prestazioni in favore dei Professionisti esterni, dei Partner e dei Fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;

e) riconoscere compensi in favore dei Professionisti esterni, dei Partner e dei Fornitori che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;

f) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;

Per consentire l'attuazione delle linee guida sin qui esposte, si procederà come ai punti seguenti:

1. i rapporti nei confronti della P.A. per le Aree a Rischio devono essere gestiti in modo unitario, procedendo alla nomina di uno o più Responsabili Interni per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse);

2. gli accordi di associazione con i Partner devono essere definiti per iscritto con l'evidenziazione di tutte le condizioni dell'accordo stesso in particolare per quanto concerne le condizioni economiche concordate per la partecipazione congiunta alla procedura – e devono essere proposti o verificati o approvati da almeno due soggetti appartenenti ad Arechi Multiservice;

3. gli incarichi conferiti ai Professionisti esterni devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito e devono essere proposti o negoziati o verificati o approvati da almeno due soggetti appartenenti a Arechi Multiservice S.p.A..;

4. i contratti stipulati con i Fornitori nell'ambito delle Aree a Rischio devono essere redatti per iscritto con l'indicazione del compenso pattuito e devono essere proposti o negoziati o verificati o approvati da almeno due soggetti appartenenti a Arechi Multiservice S.p.A..;

5. nessun tipo di pagamento può esser effettuato in contanti o in natura;

6. le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;

7. coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi l'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire tempestivamente all'Organismo Di Vigilanza eventuali situazioni di irregolarità.

SISTEMA DI CONTROLLO SULLA SALUTE E SICUREZZA SUL LAVORO.

Per ciò che concerne i rischi connessi alla salute e sicurezza sul lavoro, la Società demanda tale aspetto ai documenti periodici che andranno con il tempo ad allegarsi al presente MOGC.

L'ODV, inoltre, si fa carico di redigere con periodicità annuale dei report aventi ad oggetto l'adempimento, da parte della Società, di tutti gli obblighi giuridici relativi:

- al rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazione dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- all'acquisizione di documentazioni e certificazioni obbligatorie di legge;

- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Simili report saranno tesi:

1. all'identificazione dei rischi ed alla loro valutazione;
2. all'individuazione delle misure di prevenzione e di protezione adeguate rispetto ai rischi riscontrati, affinché questi ultimi siano eliminati ovvero, ove ciò non sia possibile, siano ridotti al minimo – e, quindi, gestiti - in relazione alle conoscenze acquisite in base al progresso tecnico;
3. alla limitazione al minimo del numero di lavoratori esposti a rischi;
4. alla definizione di adeguate misure di protezione collettiva e individuale, fermo restando che le prime devono avere priorità sulle seconde;
5. al controllo sanitario dei lavoratori in funzione dei rischi specifici;
6. alla programmazione della prevenzione, mirando ad un complesso che integri in modo coerente le condizioni tecniche e produttive dell'azienda con l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro, nonché alla successiva realizzazione degli interventi programmati;
7. alla formazione, all'addestramento, alla comunicazione ed al coinvolgimento adeguati dei destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL;

8. alla regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo alla manutenzione dei dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

La Società ha, quindi, rivolto particolare attenzione alla esigenza di predisporre ed implementare, in materia di SSL, un efficace ed efficiente sistema di controllo.

Seguendo tale protocollo la Società, sotto l'egida dell'OdV, assicurerà la più ampia tutela alla salute e sicurezza dei lavoratori, tramite l'adozione di un sistema di controllo che, anche in presenza di sopraggiunte e mutate esigenze, rimarrà vigile e costantemente aggiornato sulle aree maggiormente critiche per la materia in oggetto.