Studio Colosseo s.r.l.

Via Vescia 12 – 00183 Roma

DISPOSIZIONI PER L'UTILIZZO DEI SISTEMI INFORMATIVI E DEI SERVIZI INFORMATICI DELLA STUDIO COLOSSEO S.R.L. – PRIVACY POLICY

(Disciplinare per la protezione dei dati)

La progressiva diffusione di nuove tecnologie informatiche e dei servizi basati su di esse espone le aziende a rischi di un coinvolgimento in termini di responsabilità, sia sul piano patrimoniale che su quello penale, creando al contempo problemi di immagine e sicurezza. A quest'ultimo fine la Studio Colosseo s.r.l. Ha deciso di smaterializzare i documenti contenenti dati sensibili e con il presente disciplinare, intende fornire, idonee indicazioni ed istruzioni a tutto il personale interessato, anche nel rispetto delle linee guida del Garante della Privacy emanate con delibera n. 13 del 1 marzo 2007. Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni che saranno fornite a tutti gli incaricati in attuazione del Regolamento (U.E.) 2016/679. Il presente disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i soci e collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

Premesso

1) Che l'utilizzo delle risorse informatiche e telematiche dell'Azienda deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

2) Che ai sensi del Regolamento (U.E.) 2016/679 s'intende per:

a) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
e) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non

possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

f) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

g) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

h) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

i) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

l) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

m) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

n) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

o) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

p) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; q) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

r) «stabilimento principale»: - per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni

sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
- con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente disciplinare;

s) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente disciplinare;

t) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

u) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

v) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

w) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

x) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
- il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
- un reclamo è stato proposto a tale autorità di controllo;

y) «trattamento transfrontaliero»:

-trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
- trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

z) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente disciplinare, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente disciplinare, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai

diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

aa) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

bb) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3) Che le informazioni possono essere classificate come segue:

- Pubblica: informazione generale esplicitamente rivolta anche a comunicazione o diffusione indifferenziata all'esterno dell'Azienda (Studio Colosseo s.r.l. da ora in avanti l'Azienda)
- Comune: informazione generale da ritenersi riservata alla sola Azienda; può essere conosciuta anche da soggetti esterni purché indicati esplicitamente tra i destinatari.
- Riservata: informazione rivolta a specifici soggetti destinatari.

4) Che per trattamento dei dati (Codice Privacy) si intende "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati". In tale ottica è indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy. Pertanto le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

a) Il reperimento delle informazioni. Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi.

b) Il trattamento "interno" delle informazioni. Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili. Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione eccetera;
- l'elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti; - la selezione, la estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;
- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza; - la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

c) L'uso delle informazioni nei rapporti con l'esterno. Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della privacy altrui: essi vengono genericamente

definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta e ai trattamenti interni. L'utilizzo può essere:
- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni;
- ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.
Le operazioni di utilizzo a cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive della privacy, sono quelle con cui si mettono a disposizione di terzi i dati personali. Esse sono:
- la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

5) Che per lo svolgimento delle quotidiane attività lavorative, l'Azienda necessita in differenti ruoli e posizioni organizzative dell'utilizzo di apparecchiature informatiche. L'uso di tali apparecchiature deve essere disciplinato da norme certe in quanto da comportamenti - anche inconsapevolmente non leciti - possono derivare conseguenze gravi, sia sul piano tecnico (come un blocco della funzionalità o una perdita di dati) sia sul piano giuridico (mediante l'insorgere di responsabilità sia penali sia civili a carico contestualmente dell'Azienda e del lavoratore).

Tutto ciò premesso, si ritiene utile adottare ulteriori regole interne, dirette ad evitare che comportamenti inconsapevoli e/o scorretti possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati e, al fine, occorre che ciascun dipendente (sia esso responsabile o incaricato del trattamento) si uniformi al rispetto delle seguenti regole al fine di adempiere correttamente alle disposizioni legislative.

Allo scopo di chiarire definitivamente le norme di comportamento viene, pertanto, emanato il seguente

Disciplinare della Studio Colosseo s.r.l. per la protezione dei dati

affinché i dipendenti evitino di porre in essere inconsapevoli comportamenti incompatibili con la correttezza professionale richiesta e/o con il corretto svolgimento della prestazione lavorativa da parte degli stessi. Quanto segue è redatto nel pieno rispetto delle leggi regolatrici i rapporti di lavoro ed è pertanto indispensabile la sua conoscenza da parte di tutti i dipendenti dell'Azienda.

I SISTEMI E I SERVIZI INFORMATICI

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro e ogni utilizzo non inerente l'attività lavorativa è vietato. Tale utilizzo, inoltre, può contribuire ad innescare disservizi, costi di manutenzione aggiuntivi per azioni scorrette e minacce alla sicurezza e pertanto:

• le attrezzature informatiche vanno custodite in modo appropriato ed esclusivamente circoscritto alle attività lavorative cui ciascuno è preposto;

• le attrezzature informatiche non possono essere autonomamente spostate o trasferite poiché l'assegnazione all'utente della postazione di lavoro è registrata su apposita scheda contenente l'identificativo dell'utente, le matricole delle attrezzature assegnate, le configurazioni hardware e software unitamente ad altri dati per la gestione delle attrezzature stesse;

• tali strumenti possono essere utilizzati solo per fini aziendali (in relazione ovviamente alle mansioni assegnate) e non anche per scopi personali, in quanto ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla

sicurezza. Una condotta non conforme a tale prescrizione potrebbe comportare sanzioni disciplinari a carico del contravventore;

• il furto, il danneggiamento o lo smarrimento di attrezzature informatiche deve essere prontamente segnalato alle strutture competenti;

Qualora la strumentazione data in uso al dipendente venga usata per scopi personali durante l'orario di lavoro o per commettere illeciti o condotte che possano causare danni all'Azienda (quali la navigazione su siti di scommesse on line, siti pornografici, o pedo-pornografici, la diffusione di notizie riservate, etc.), su autorizzazione dell'Amministratore della società, verrà effettuato un richiamo generale, individuando inizialmente solo l'area e non il singolo dipendente. Tale controllo anonimo si concluderà con avvisi generalizzati relativi ad eventuali rilevazioni di utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. In assenza di reiterazione di tali condotte non verranno effettuati altri controlli; nel caso contrario, su autorizzazione dell'Amministratore, verranno inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni e a, seconda della gravità della violazione perpetrata, sarà prevista una sanzione secondo quanto disposto dal Codice Disciplinare dell'Azienda.

Resta sempre salvo l'obbligo dell'Azienda di comunicare i log file contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle autorità competenti. Le eventuali attività di monitoraggio relative alle attività di navigazione e di utilizzo degli strumenti informatici, al fine di prevenire utilizzi indebiti degli strumenti stessi, che possono essere fonte di responsabilità per l'Azienda, saranno svolte solo con l'autorizzazione dell'Amministratore e da soggetti a ciò preposti e saranno strettamente mirate sull'area di rischio individuata. Il personal computer dato in affidamento all'utente permette l'accesso al Server interno dell'Azienda solo attraverso specifiche credenziali di autenticazione. La parola chiave individuale, comunicata dall'Azienda ed associata alla credenziale di autenticazione, deve essere custodita e non divulgata; tale credenziale consente a ciascun incaricato il primo accesso al sistema informativo. Essa dovrà tuttavia essere immediatamente modificata attraverso la scelta di una parola chiave di 8 caratteri alfanumerici che non contenga riferimenti alla sua persona. Qualora l'utente prenda coscienza che taluno può aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente cambiarla.

In particolare le password di accesso ai servizi di rete devono:

a) essere costituite da almeno 8 caratteri;

b) contenere un set di caratteri il più possibile esteso (oltre ai caratteri dell'alfabeto, quelli numerici e quelli speciali ad esempio |!"£$%&/()=?^*+[ç@#°§_-:.;,<>\]);

c) non essere banali: cioè reperibili in dizionari on-line, non facilmente associabili alla persona; non essere ripetizione della login o una permutazione ciclica della login, né una stringa di caratteri contigui della tastiera.

d) contenere caratteri maiuscoli e/o minuscoli;

e) essere cambiate dall'operatore subito all'atto della prima assegnazione e, successivamente, sulla base della policy adottata dall'Aziende, con cadenza semestrale, a meno di conseguente blocco dell'account, evitando il riutilizzo di chiavi già adottate nei 12 mesi precedenti. Nella configurazione delle caselle di posta elettronica non devono essere utilizzate le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni. E' vietato riutilizzare la propria password aziendale per la registrazione in altri siti web.

Installazione dei programmi e utilizzo del personal computer

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli qui di seguito richiamati a titolo indicativo.

a) onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, l'installazione dei programmi deve sempre essere effettuata dai tecnici informatici preposti, dietro autorizzazione dell'Amministratore;

b) non è consentito l'uso di programmi non distribuiti ufficialmente dalle società che ne detengono i diritti (si vedano in proposito, gli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del software e dalla l. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore);

c) non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

d) non è consentita l'installazione sul proprio PC di apparati di comunicazione propri (come ad esempio modem, hard-disk, chiavette per connessione internet, ecc..);

e) non è consentito scaricare e duplicare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa;

f) non è consentito detenere sul proprio PC software non aventi alcuna attinenza con l'attività lavorativa;

g) non è consentito detenere sul proprio PC software reperiti in rete o da qualunque altra sorgente esterna, salvo espressa autorizzazione da parte dell'Azienda: tutti i file di provenienza incerta o esterna, infatti, ancorché attinenti all'attività lavorativa, devono essere sottoposti ad un attento controllo;

h) sui PC dotati di scheda audio e/o di lettore CD/DVD non è consentito l'ascolto di programmi, files audio o musicali, visualizzazione di filmati, se non a fini prettamente lavorativi.
L'Amministrazione si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema, ovvero acquistati o installati in violazione delle presenti disposizioni (a titolo esemplificativo e non esaustivo, tutti i file non pertinenti all'attività lavorativa tipo MP3, AVI; MPEG; ecc..).

Poiché in caso di violazioni contrattuali e giuridiche sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Azienda verificherà, nei limiti consentiti dalla legge, il rispetto delle regole e l'integrità del proprio sistema informatico. A tal fine l'Azienda si potrà avvalere di informazioni fornite da soggetti che, in esecuzione di rapporti contrattuali, intervengono sul Sistema Informativo in qualità di titolari autonomi o Responsabili esterni. Qualora, a seguito di controllo sul PC in uso all'utilizzatore, dovuto a ragioni manutentive, risulti presente software non espressamente autorizzato dall'Amministrazione, saranno posti in essere richiami disciplinari, motivati dal fatto che qualsiasi programma estraneo a quelli contenuti e autorizzati dalla stessa Amministrazione può cagionare incompatibilità con i programmi forniti e già in uso per lo svolgimento dell'attività e/o costituire una minaccia per la sicurezza informatica. Il Personal Computer deve essere spento (salvo specifiche esigenze tecniche asseverate dal proprio Responsabile) o bloccato ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Va comunque adottata la modalità savescreen a tempo con obbligo di reintrodurre la password per l'accesso, modalità che evita di lasciare incustodito il PC, anche in caso di mancato spegnimento da parte dell'utente.

Utilizzo di supporti di memorizzazione

Per quanto riguarda i supporti di memorizzazione:

a) non è consentito scaricare files contenuti in supporti di memorizzazione non aventi alcuna attinenza con la propria prestazione lavorativa;

b) ogni dispositivo magnetico di provenienza esterna dall'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'Amministratore di Rete;

c) tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti ad attento controllo. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte delle strutture centrali. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente. Tutti i supporti di memorizzazione rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. A tal fine, queste informazioni non devono essere archiviate su supporti rimovibili oltre il tempo strettamente necessario, terminato il quale devono essere cancellate.

Utilizzo della rete aziendale

Le cartelle di rete sono aree di condivisione di informazioni strettamente aziendali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque files che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste cartelle. E' fatto divieto di far circolare internamente alla rete aziendale file non espressamente autorizzati, né software non forniti dall'Azienda, né alcun altro documento o notizia, informazione o dato non inerente all'attività aziendale. L'Azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Disciplinare e/o comunque di norme di Legge (a titolo esemplificativo e non esaustivo tutti i files non pertinenti l'attività lavorativa e di tipo MP3, AVI, MPEG, ecc.). L'utente è responsabile di un utilizzo delle risorse informatiche e delle informazioni compatibilmente con gli scopi dell'Azienda e nel rispetto del presente Disciplinare. In particolare l'utente ha a disposizione una cartella personale alla quale accede come unico utente e le cartelle della propria area di appartenenza per la condivisione dei file di lavoro. Le eventuali attività di monitoraggio, al fine di prevenire utilizzi indebiti della rete o degli strumenti informatici, che possono essere fonte di responsabilità per l'Azienda, saranno svolte solo da soggetti a ciò incaricati, e saranno mirate all'area di rischio individuata.

Gestione, conservazione e controllo dei dati informatici

È fatto divieto di applicare sistemi di crittografia ai dati o comunque altri sistemi che rendano difficile o impossibile la lettura dei documenti, se non espressamente autorizzati per iscritto dall'Azienda potrà comunque adottare procedure informatiche, che siano adeguate a garantire per determinate banche dati e/o cartelle e/o aree di server una particolare sicurezza informatica anche attraverso processi di crittografia.

Gestione, conservazione e archiviazione della documentazione e dei dati informatici del dipendente in corso di pensionamento

In caso di pensionamento, il referente informatico è incaricato, di procedere con le misure di sicurezza necessarie. L'amministratore in via di pensionamento è tenuto a comunicare a tutto il personale, con foglio d'ordine, prima della data di pensionamento, chi vada contattato in

sostituzione dello stesso (nominativo, collocamento, numero di telefono e indirizzo e-mail) a partire dal giorno successivo a quello del pensionamento. Inoltre, entro la data di pensionamento, lo stesso dirigente provvede a far sì che:

- gli archivi cartacei, come pure tutta la documentazione cartacea, vengano dati in consegna agli stessi soggetti individuati in sostituzione del dipendente uscente. Se nel giro di 6 mesi non provvede a tale passaggio di consegna, gli archivi/i documenti vengono cancellati salvo che non comunichi la necessità di mantenerli. In tal caso spetta all'Amministratore stesso prenderli in consegna;
- gli archivi informatici come pure tutta la documentazione informatica, informandone il settore informatico, vengano attribuiti in rete (sul server), analogamente a quanto sopra, agli stessi soggetti individuati in sostituzione del dipendente uscente. Se nel giro di 6 mesi non vi provvede, gli archivi/i documenti vengono cancellati salvo che non comunichi la necessità di mantenerli. In tal caso spetta all'Amministratore stesso prenderli in gestione. Sempre entro la data di pensionamento, l'Amministratore inoltre incarica il dipendente uscente di trasmettere i contenuti delle e-mail di lavoro, considerate utili, ai soggetti che lo sostituiranno o allo stesso Amministratore, stando che una volta in pensione, la sua cartella di posta elettronica non sarà più accessibile per nessuno. Il settore informatico, quindi, entro il primo giorno di pensionamento, attribuirà, sul server, le cartelle informatiche ed i files ai destinatari individuati dall'Amministratore tramite il foglio d'ordine sopra citato. Diversamente le conserverà per 6 mesi e poi procederà alla cancellazione. Inoltre, il primo giorno di pensionamento, il settore informatico archivierà la gestione delle e-mail del dipendente in pensione e attiverà una e-mail automatica, per un tempo massimo di 6 mesi, informando tutti coloro che dovessero ancora scrivergli, che il dipendente è in pensione e quell'indirizzo e-mail non è più utilizzabile. In tale risposta automatica deve essere indicato l'indirizzo di email a cui inviare eventuali comunicazioni. Trascorsi 6 mesi, la cartella di posta elettronica del dipendente in pensione verrà cancellata.

Utilizzo della rete Internet e dei relativi servizi

1 Navigazione in Internet

a) non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, in quanto l'utilizzo al collegamento ad Internet deve essere funzionale all'attività lavorativa. Una violazione di tale prescrizione potrebbe comportare sanzioni disciplinari a carico del contravventore. Qualora vengano perpetrati eventuali illeciti nella navigazione in internet, su autorizzazione dell'Amministratore, verrà individuata inizialmente solo l'area oggetto dell'illecito e non il singolo dipendente. Tale controllo anonimo si concluderà con avvisi generalizzati relativi ad eventuali rilevazioni di utilizzo anomalo degli strumenti regionali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. Tale avviso sarà inizialmente circoscritto a dipendenti afferenti all'area o al settore in cui è stata rilevata l'anomalia; in assenza di successive anomalie non verranno effettuati altri controlli, in caso contrario su autorizzazione dell'Amministratore, si procederà con controlli su base individuale per risalire al colpevole. A seconda della gravità della violazione perpetrata la sanzione prevista sarà quella prevista dal Codice Disciplinare dell'Agenzia. Come precedentemente indicato, resta sempre salvo l'obbligo dell'Azienda di comunicare i log file contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle autorità competenti;

b) non è consentita l'effettuazione di ogni genere di transazione finanziaria, acquisti on-line e simili, salvo i casi direttamente autorizzati e nel rispetto delle normali procedure di acquisto. E' invece consentito un limitato utilizzo di funzionalità di home banking, per piccole necessità personali ed entro limiti di accettabilità e correttezza;

c) non è consentito il download di software gratuiti (freeware) e shareware prelevato da siti Internet,

se non pertinenti l'attività lavorativa;

e) è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

f) non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);

g) non è consentito l'uso di Internet per la ricezione di programmi radio e musicali, per conversazioni in chat line o collegamenti a webcam, ad eccezione di motivi professionali preventivamente autorizzati per iscritto dall'Azienda;

h) non è consentito il trattamento di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

A fronte di quanto sopra indicato come regole sulla navigazione Internet, inoltre, si informa che tutto il traffico viene registrato su log che non vengono direttamente analizzati, ma conservati in modo che possano essere messi a disposizione, se ufficialmente richiesto, dell'autorità giudiziaria e/o di polizia a fine di indagini.

Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, l'Azienda, su autorizzazione dell'Amministratore, adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure già in precedenza specificate. Si rende noto che l'Azienda può, in seguito al rilevamento di anomalie nel sistema dei dati o in caso di comportamenti anomali individuati in una determinata area, su autorizzazione dell'amministratore, attivare meccanismi di monitoraggio delle attività di accesso internet (file di log) per verifiche sulla funzionalità del sistema o di controllo della sicurezza dell'impianto. Gli archivi di log risultanti da questo monitoraggio, effettuati in determinate aree dell'azienda e allo stesso tempo sufficientemente grandi da garantire la riservatezza dei lavoratori, contengono traccia di ogni operazione di collegamento effettuata dall'interno dell'Azienda verso Internet. Le informazioni relative alle componenti di file di log eventualmente registrati sono memorizzate temporaneamente e vi può accedere solo personale appositamente incaricato. Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Nel caso di anomalie o per prevenire situazioni di pericolo o eventi dannosi, l'Azienda, su autorizzazione dell'Amministratore, effettuerà un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue determinate aree. Tale controllo anonimo si concluderà con avvisi generalizzati relativi ad eventuali rilevazioni di utilizzo anomalo degli strumenti regionali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. Tale avviso sarà inizialmente circoscritto a dipendenti afferenti all'area o al settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non verranno effettuati altri controlli; nel caso di abusi singoli o reiterati, su autorizzazione dell'Amministratore, verranno inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni.

2 Posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:
a) non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo

svolgimento delle mansioni assegnate;

b) non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

c) la posta elettronica può essere intercettata da estranei, e dunque, non deve essere usata per inviare documenti di lavoro "Strettamente Riservati"; in casi particolari e motivati, ma comunque solo subordinatamente all'ottenimento della preventiva autorizzazione scritta, sarà possibile il ricorso alla crittografia;

d) non è consentito il reindirizzamento automatico della corrispondenza verso indirizzi non aziendali;

e) non è consentito l'utilizzo, per motivi non attinenti l'attività lavorativa, dell'indirizzo di posta elettronica aziendale (@studiocolosseo.com) per la partecipazione a dibattiti, Forum o mail-list, salvo diversa ed esplicita autorizzazione,

f) la casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Stante la natura di strumento lavorativo del sistema di posta elettronica, il dipendente è quindi consapevole che su tale strumento di comunicazione non potrà essere garantita la riservatezza dei documenti inviati e ricevuti; pertanto, sarà impegno del dipendente evitare l'utilizzo delle caselle di posta aziendali per comunicazioni di carattere personale o che esulino dal contesto dell'Agenzia. Poiché in caso di violazioni contrattuali e giuridiche, sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. A tal fine l'Azienda si potrà avvalere di informazioni fornite da soggetti che, in esecuzione di rapporti contrattuali, intervengono sul Sistema Informatico aziendale in qualità di titolari autonomi o responsabili esterni. L'Azienda, pertanto, avvalendosi della facoltà di effettuare i c.d. "controlli difensivi" potrà, su autorizzazione dell'Amministratore, saltuariamente, e solo in caso di stretta necessità, effettuare controlli sull'area del traffico dati della posta elettronica aziendale, esclusivamente per finalità di difesa e tutela del patrimonio aziendale. In nessun caso verrà effettuato l'accesso diretto alla casella di posta elettronica aziendale dei dipendenti, se non in seguito a gravi e comprovati motivi che possano rilevare il compimento di reati o condotte illecite oppure su segnalazione dell'Autorità Giudiziaria nell'ambito di indagini svolte per la repressione, accertamento e prevenzione di reati.

Inoltre, si comunica che ciascun dipendente, in caso di assenza per qualsiasi motivo (ferie, allontanamento temporaneo dal posto di lavoro, malattia) e al fine di non interrompere né rallentare i processi produttivi e/o lavorativi, ha la facoltà di inserire nel proprio account di posta elettronica la funzione di risposta automatica, contenente le coordinate di altri lavoratori a cui rivolgersi in sostituzione del dipendente assente; il delegato potrà in questo modo ricevere i messaggi di posta elettronica del dipendente assente e a lui indirizzati.

Custodia, conservazione e controllo documenti cartacei

E' fatto obbligo al dipendente di: -

custodire il materiale cartaceo contenente dati personali e aziendali affinché nessuno ne prenda visione, possa manipolarlo o riprodurlo;

- custodire il materiale cartaceo contenente dati personali sensibili in archivi dotati di chiusura a chiave;

Precisiamo che nella nostra Azienda l'uso di documentazione cartacea è estremamente limitata ai

casi previsti dalla legge. I documenti cartacei sono conservati in apposito armadio chiuso a chiave il cui accesso è regolato dal responsabile trattamento dati personali dell'Azienda.

- non lasciare documenti incustoditi presso la propria postazione qualora sia previsto un allontanamento per un lasso di tempo tale da consentirne eventualmente la visione da parte di terzi;

- non lasciare qualsiasi documento in locali estranei alla propria postazione, prestando particolare attenzione a non lasciarli presso la fotocopiatrice.

Utilizzo del fax, telefono, cellulare e fotocopiatrici

Il telefono, il cellulare aziendale e le fotocopiatrici devono essere utilizzati per scopi strettamente connessi all'attività lavorativa. L'utilizzo per qualsiasi altro scopo potrà essere oggetto di sanzioni disciplinari e, a seconda della gravità della violazione perpetrata, la sanzione prevista sarà quella prevista dal Codice Disciplinare dell'Azienda.

Non è consentito rivelare numeri telefonici interni o informazioni sulla struttura aziendale a persone non positivamente identificate. È fatto divieto di lasciare documenti incustoditi presso le postazioni o presso i locali delle fotocopiatrici. Non è consentito lasciare messaggi contenenti password o informazioni riservate su alcuna segreteria telefonica e si deve sempre informare l'interlocutore se si sta utilizzando la modalità "viva voce". Ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari che potranno variare a seconda della gravità (come sopra specificato).

Registrazione, conservazione e analisi degli access log (autenticazioni informatiche) degli Amministratori di Sistema

Si rende noto che la Studio Colosseo s.r.l. deve - in ottemperanza alle disposizioni contenute nel Provvedimento del Garante della Privacy del 27 Novembre 2008 recante "Misure e accorgimenti, prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e successive modificazioni

- attivare, su autorizzazione dell'Amministratore, meccanismi di controllo (almeno annuali) delle attività degli Amministratori di Sistema, in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. In particolare, viene verificato che le attività svolte dall'amministratore di sistema siano conformi alle mansioni attribuite mediante lettera di nomina.

A tal fine, l'Azienda si è dotato di un sistema idoneo alla raccolta degli accessi logici (autenticazione informatica) ai sistemi di elaborazione (client, server, apparati di sicurezza, apparati di rete ecc…) e agli archivi elettronici (file, database, posta elettronica, gestionali, ERP, log ecc…) effettuati da parte degli amministratori di sistema. Tali registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste, ovvero per verificare eventuali abusi e/o violazioni della riservatezza dei dati da parte di amministratori di sistema. E' pertanto esclusa la finalità, anche indiretta, del controllo dei lavoratori. Gli archivi di log (ovvero degli access log) risultanti da questo monitoraggio e attività di verifica (accessi, tentativi di accesso, disconnessioni ai sistemi di elaborazione, intesi sia come server che client, a software e data base), contengono traccia di alcune operazioni effettuate dagli amministratori di sistema. Le informazioni relative alle

componenti di file di log eventualmente registrati sono memorizzate e conservate temporaneamente (per una durata minima di 6 mesi) e vi può accedere solo il Titolare, eventualmente per il tramite di una persona appositamente incaricata.

Segreto d’ufficio

Il dipendente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in tutto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Nella valutazione delle informazioni, il dipendente si impegna a prendere ogni misura perché le stesse rimangano segrete, essendo inteso che, in caso di divulgazione non autorizzata, sarà a carico del dipendente l'onere di provare di avere adottato tali misure. Il dipendente si impegna a rispettare con esattezza i suddetti obblighi poiché si presume che la violazione degli impegni di segretezza contenuti nel presente disciplinare siano idonei a causare ingenti danni all’Azienda. Gli obblighi del dipendente previsti in questo capo non termineranno all’atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che lo stesso possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

Applicazione ed interpretazione del presente disciplinare

Per qualsiasi dubbio relativo all’applicazione pratica o all’interpretazione del presente disciplinare, il dipendente può rivolgersi al Responsabile Trattamento dati personali dell'Azienda che si avvale della collaborazione dell'Amministratore di rete per i contenuti di competenza dello stesso.

Disciplina relativa a deroghe e modifiche del presente disciplinare

Qualora il Comune intenda apporre modifiche alle presenti disposizioni, queste saranno applicate dandone conoscenza immediata al dipendente mediante apposita comunicazione e sulla Intranet. Qualora si renda necessario per qualsiasi motivo, derogare ad uno o più punti delle presenti disposizioni, salvo i casi in cui le deroghe siano espressamente previste e regolamentate nello stesso disciplinare, sarà obbligatorio porre per iscritto e veder accettata dal dipendente e dall’Azienda tale deroga mediante sottoscrizione di entrambe.

Deroghe o modifiche di uno o più punti del presente disciplinare, non rendono invalidi gli altri punti, salvo ipotesi di evidente incompatibilità, per cui prevarrà l’applicazione della clausola temporalmente più recente.

Eventuali comportamenti non in linea con il presente disciplinare, che venissero comunque tollerati dall’Azienda, non costituiscono una rinuncia dell’Azienda stessa ad esercitare successivamente i suoi diritti per far valere il presente disciplinare. La non osservanza delle presenti disposizioni può comportare sanzioni disciplinari, civili e penali. A seconda della gravità della violazione perpetrata la sanzione disciplinare prevista è quella prevista dal Codice Disciplinare dell'Azienda.

Il presente Disciplinare è soggetto a revisione con frequenza annuale.

Roma 12 Novembre 2020

Marco Manieri