G.D.P.R. – UE 2016/679

REGOLAMENTO GENERALE PER LA PROTEZIONE DEI DATI

Codice Deontologico Aziendale

SITEM S.r.l.

Via Della Costa, 6 – 67047 Rocca Di Cambio (AQ)

P. Iva 01326320668

Premessa

Il Codice Deontologico Aziendale è quel documento che indica come lo Studio ha deciso che ci si debba comportare nei confronti dei trattamenti di dati personali.
Il G.D.P.R. ha notevolmente modificato le abitudini quotidiane introducendo obblighi e comportamenti a prima vista complessi da rispettare.
Il Codice Deontologico Aziendale intende, nel rispetto di quanto previsto dal G.D.P.R., guidare ed aiutare gli incaricati a gestire le operazioni quotidiane relative ai trattamenti effettuati principalmente con l'ausilio di PC individuali e con supporti cartacei. Indica:

- Le modalità generiche di utilizzo degli strumenti individuali informatici dati in concessione ai dipendenti e collaboratori aziendali, fornendo indicazioni comportamentali al fine di evitare di incorrere nei rigori legislativi.
- I comportamenti da tenere da parte dei dipendenti e collaboratori aziendali per i trattamenti effettuati con e senza l'ausilio di strumenti informatici.

Il suo rispetto è obbligatorio, ogni incaricato è tenuto al rispetto di quanto indicato pena il diritto da parte dello Studio di richiedere giusto risarcimento per i danni materiali e immateriali subiti, la segnalazione alle autorità inquirenti per l'eventuale ipotesi di reati penali oltre all'eventuale recessione contrattuale.

La legge sulla privacy.

La legge esiste dal 1996, prima D.Lgs. 675, poi D.Lgs. 196/03 e dal 25/06/2016 G.D.P.R. UE 2016/679. Essa tutela l'uso delle informazioni stabilendo delle regole ferree ma al contempo tali da permettere duttili comportamenti; sinteticamente si può affermare che nulla è proibito ma tutto é regolamentato.
Questo significa che non esistono operazioni proibite sui dati personali ma ogni operazione deve sottostare a regole che innanzitutto prevedano che l'interessato (colui a cui si riferiscono i dati) sappia esattamente cosa si fa delle proprie informazioni e possa in ogni momento verificare quanto detto.
Chi non rispetta i vincoli legislativi rischia di incorrere in gravi conseguenze sia sul piano economico che penale.
Il G.D.P.R. con l'articoli 1 comma 2 (Il presente Regolamento protegge i diritti e le libertà fondamentali delle persone fisiche che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, in particolare il diritto alla protezione dei dati personali.) dichiara apertamente di essere una norma comportamentale, una norma che oltre a dettare regole precise, gestisce anche i rapporti tra le persone.
L'uso della tecnologia, soprattutto l'Information Tecnology, ha cambiato

velocemente la società.
Avere informazioni è oggi di vitale importanza e l'aumento e il miglioramento della tecnologia ha portato ad un incremento esponenziale di informazioni, dalle più banali alle più complesse, che circolano in internet.
Per evitare abusi e ingerenze nella sfera privata delle persone sono nate leggi che regolamentano la condivisione delle informazioni e che indicano comportamenti e regole necessarie a garantire gli interessi di tutti, ma, in primis, a salvaguardare l'uomo.
Ed è in quest'ottica che il legislatore Europeo e i legislatori dei singoli Stati Comunitari si adoperano, promulgando sempre nuove norme per la protezione dei dati personali.
Non è semplice rispettare la legge ma alcune regole di base, evidenziabili dagli articoli del G.D.P.R., possono aiutare gli interessati ad operare con una certa dose di sicurezza, ricordando sempre che, come nel settore della sicurezza personale, ogni individuo con il proprio comportamento è parte attiva e fondamentale nell'intero processo aziendale del trattamento delle informazioni.
Per questo motivo lo Studio si è dotato di un codice etico e di linee guida a cui tutti gli incaricati devono sottostare e che sono indicate in questo documento.
È necessario definire alcuni termini per rendere la norma comprensibile :

- 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.
- 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.
- 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.
- 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.

- 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.
- Incaricato : Le persone fisiche autorizzate a compiere i trattamenti.
- Interessato : La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati.
- Comunicazione : 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.
- Diffusione : Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- 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;

Il trattamento è un insieme di attività sui dati che ha un inizio ed una fine facilmente identificabili.
Ad esempio:

- la rubrica dei clienti che si utilizza per generare lettere circolari tramite un word processor è una trattamento che ha inizio nel momento in cui si decide di creare la rubrica e termina nel momento in cui la si cancella fisicamente dal computer;
- il foglio di calcolo (o il blocchetto di carta) usato per registrare giornalmente le telefonate ricevute indicando informazioni identificative dell'interlocutore, ha inizio con la prima registrazione e termina con la cancellazione del foglio dal computer o distuggendo il blocchetto di carta.

Si è detto che questa norma non proibisce ma regolamenta i trattamenti e per fare ciò detta alcune regole fondamentali che ogni trattamento deve rispettare, indipendentemente dal fatto che il trattamento nasca da un obbligo legislativo o esigenza lavorativa ed indipendentemente dal fatto che sia svolto con l'ausilio di strumenti informatici o cartacei.
Quindi affinché un trattamento sia lecito deve utilizzare dati:

- raccolti e registrati per scopi determinati, espliciti, legittimi e sempre

aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Il mancato rispetto rende di fatto un trattamento da lecito a illecito con gravi conseguenze per lo Studio e l'incaricato.

Codice Deontologico dello Studio

Lo Studio, in qualità di Titolare, adotta il seguente codice deontologico impegnandosi a garantire, con ogni mezzo, che il trattamento delle informazioni detenute sia sempre leale e corretto.

- Lo Studio, ritenendo il rapporto con i propri clienti, fornitori e collaboratori fondamentale per la propria esistenza, adotta tutte le misure a salvaguardia delle informazioni trattate, indipendentemente dagli strumenti usati.
- Solo i trattamenti che hanno ottenuto l'avallo del Titolare sono effettuati dallo Studio.
- Sono banditi tutti i comportamenti e strumenti che tramite il trattamento di informazioni possono ledere i diritti dei singoli individui.
- Gli Incaricati vengono istruiti, oltre che sulla legge, sui motivi che hanno permesso la realizzazione della legge per la protezione dei dati personali.
- Ogni Incaricato tratta solo ed unicamente le informazioni per le quali ha ricevuto incarico da parte del Titolare.
- Ogni Incaricato nel trattare verbalmente le informazioni adotta atteggiamenti di "cortese riservatezza" verso i propri interlocutori al fine di non diffondere informazioni conosciute.
- Ogni Incaricato applica il "segreto professionale" ad ogni informazione trattata indipendentemente dagli obblighi legislativi.
- Ogni Incaricato è parte attiva del sistema di sicurezza sulle informazioni adoperandosi affinché siano garantiti i diritti sanciti e rispettate le regole stabilite.
- Ogni Incaricato si fa garante, per la propria competenza, dell'esattezza e correttezza delle informazioni trattate.
- Nel ricevere i Clienti e /o informazioni dagli stessi, ogni Incaricato si adopera per garantire la massima riservatezza, adoperandosi in modo attivo anche dove lo Studio non ha ancora previsto sistemi idonei a

garantire il diritto di riservatezza.
- Ogni Incaricato si fa parte attiva a diffondere presso i Clienti dello Studio i precetti base della normativa sulla protezione dei dati personali.

Per mettere in pratica questi precetti sono di seguito riportate le istruzioni per i trattamenti con l'utilizzo degli strumenti informatici (gestione dei dati raccolti, per il mondo internet, per le mail) e per i trattamenti manuali.

TRATTAMENTI INFORMATICI

Custodia degli strumenti.

I Personal Computer (fissi o mobili), con i relativi programmi, le applicazioni e le configurazioni sono registrati su una apposita scheda PC. Essi sono strumenti di lavoro e sono affidati all'incaricato per l'adempimento dei doveri contrattuali, pertanto tali strumenti vanno custoditi in modo appropriato con la dovuta diligenza e comunque in modo da evitare ogni possibile danno o deterioramento. E' consentito quindi il solo uso per fini professionali e non personali, né tanto meno per scopi illeciti.
Ai fini sopra esposti sono vietate tutte le azioni che possono ledere in modo permanente o definitivo gli strumenti e prodotti dati in utilizzo. E' anche vietato agire modificando le configurazioni degli strumenti.

Presidio degli strumenti.

Gli strumenti informatici permettono l'accesso alle informazioni detenute presso lo Studio; tali informazioni sono protette e sono trattate solo ed unicamente per determinati scopi. Tra questi non è prevista la "diffusione". Lasciare il PC attivo ed incustodito, quindi a disposizione di terzi, concretizza l'atto di diffusione dei dati. Tenendo comunque conto dell'operatività quotidiana, gli incaricati sono tenuti a:
- Chiudere la sessione quando si prevede di stare assenti per oltre dieci minuti ed è possibile la presenza di persone estranee allo Studio nei locali di lavoro (nel caso si posseggano dati *relativi alla salute* la sessione va chiusa ogni qual volta ci si assenti).
- Spegnere il PC alla fine della giornata.

Uno dei fondamenti della sicurezza è *non fidarsi.* Nella salvaguardia dei rapporti interpersonali, è consigliato adottare ogni precauzione anche verso i propri colleghi.

Autorizzazione all'uso (utente e password).

Il Titolare dei trattamenti concretizza l'autorizzazione all'uso degli strumenti informatici dotando l'incaricato di una chiave di accesso.
Tale chiave è costituita da due serie di numeri e lettere, una chiamata identificativo utente o userid che identifica il nome dell'utente, l'altra password che è una chiave segreta, non visibile quando digitata, che abbinata alla userid identifica in modo univoco l'utente.
La password è segreta, viene comunicata dal Titolare in modo riservato e diretto.
L'utente deve averne massima cura , non deve comunicarla ad altri e deve agire in modo che nessuno ne possa venire a conoscenza.
L'eventualità o il sospetto che la segretezza della password sia stata compromessa va immediatamente segnalata al Titolare che provvederà immediatamente a generarne una nuova.
Per obbligo legislativo le password hanno una durata limitata (massimo sei mesi) per cui è previsto un sistema di scadenza automatico. Ogni password scaduta non può più essere utilizzata.
La generazione delle password avviene con mezzi automatici secondo quanto previsto dal Codice.
Secondo la normativa e dottrina vigente l'uso di identificativo utente e password corrisponde ad una firma, quindi le azioni effettuate possono essere attribuite alla persona assegnataria dell'identificativo.

Accesso agli strumenti.

Per poter accedere agli strumenti del PC è necessario qualificarsi attraverso l'immissione della userid e password.
La fase di riconoscimento è suddivisa in due tempi distinti:

- All'atto dell'accensione del PC come prima attività viene richiesta l'immissione di una password. Immettere tale password che è stata consegnata. La mancata immissione o l'immissione errata, impedisce l'uso fisico dello strumento, il quale non può completare le operazioni di attivazione iniziale.
- Terminata la fase di attivazione iniziale viene caricato il Sistema Operativo, tipicamente Windows®, che richiede una nuova identificazione per poter essere completato. Immettere l'identificativo utente e la password corrispondente; la mancata o errata immissione impedisce l'uso dei programmi installati.

L'immissione di una password errata per tre volte comporta la disabilitazione del profilo o dello strumento PC. Nel caso comunicare immediatamente l'evento al Titolare.

Licenze d'uso.

I computer per il loro funzionamento si basano su programmi, ovvero su particolari archivi contenenti istruzioni; tali programmi hanno scopi diversi, servono per:

- la contabilità,
- la gestione dei magazzini,
- la creazione di testi, eseguire calcoli od analisi su dati,
- usare internet,
- lo scambio di messaggi elettronici (e_mail),
- permettere l'uso degli strumenti fisici,
- …….

Lo Studio utilizza solo ed unicamente prodotti licenziati e quindi legittimamente detenuti oppure programmi in licenza GPL (General Public License) che per loro natura e volontà degli sviluppatori non possono essere vincolati in alcun modo e sono quindi di libero possesso.
L'utilizzo di programmi non lecitamente acquisiti e/o licenziati è proibito. Raffigurando ciò un reato penale, oltre che fiscale, lo Studio si riserva il diritto di dare specifica segnalazione all'autorità giudiziaria per le proprie competenze.
Nonostante il divieto, potendo materialmente ogni incaricato, anche involontariamente, installare programmi non autorizzati, per salvaguardare gli operatori, lo Studio provvederà ad effettuate ispezioni di controllo sulle dotazioni informatiche confrontando il contenuto della scheda PC con quanto installato al momento.
La non corrispondenza tra quanto dichiarato nella scheda PC e quanto rilevato in fase di ispezione è a carico dell'incaricato il quale sarà tenuto a darne giustificazione, pena l'ipotesi di reato.
Gli operatori che necessitano l'installazione di speciali programmi dovranno farsi autorizzare dal Titolare che provvederà anche ad aggiornare la scheda del PC.

Installazione e/o cancellazione prodotti.

L' installazione o eliminazione di programmi da un sistema informatico può rompere le correlazioni tra le applicazioni e danneggiare anche gravemente il Personal Computer oltre a rendere inutilizzabili, temporaneamente o permanentemente, le funzioni.
L'interruzione temporanea o permanente delle funzioni di un sistema informativo è un grave reato penale oltre che fonte di gravi perdite economiche.
Lo Studio si riserva tutti i diritti ad agire contro chi opera interrompendo le funzioni del sistema informativo.
L' installazione di prodotti sui PC è opera del Titolare (o suo incaricato) che è

l'unico dotato di tutte le informazioni e capacità tecniche per assolvere al bisogno.
L'eventuale involontaria installazione di prodotti e/o funzioni quali plug-in ricevuti da internet, deve essere immediatamente segnalata al Titolare. La mancata segnalazione farà considerare atto volontario l'installazione con le conseguenze indicate.
Nonostante le attenzioni e i sistemi di sicurezza attivati è possibile che si installino programmi che modificano l'equilibrio del sistema per cui deve essere immediatamente segnalata al Titolare ogni variazione comportamentale degli strumenti in dotazione, tale atto impedirà l'ipotesi di reato.
Per motivi di sicurezza è proibita l'installazione sia di sottofondi al desktop di Windows ® che di screen saver se non autorizzati

Protezione informatica.

Per attacco si intende un'azione atta a rendere temporaneamente o definitivamente inservibile il PC o sue parti; si intende anche un atto tendente a eseguire operazioni non volute sul PC o suoi contenuti.
Diverse sono le tipologie di attacco che può subire un sistema informatico.
Ne elenchiamo alcune tra le più ricorrenti:

- Virus : Programmi che impediscono l'uso del computer danneggiando parte del Sistema Operativo e a volte anche creando danni fisici quale la distruzione dei dischi.
- Backdoor : Programmi che creano un collegamento nascosto tra il PC e un computer presente sulla rete internet, permettendo al proprietario del computer esterno di agire intimamente nel PC infettato.
- Spamming : Invio di messaggi e-mail senza alcun valore ma con l'intenzione di creare traffico inutile saturando le linee di comunicazione e i dischi.
- DoS : (Denial of Service) L'invio di messaggi su rete internet verso computer presenti su internet con l'intento di saturarli.
- Spoofing : Programmi atti a controllare il traffico di dati sul PC.
- Keylogger : Programmi capaci di intercettare ogni battuta fatta sulla tastiera per inviare i dati raccolti a particolari server con intenti tra i più svariati.
- Phishing : Tipo di truffa via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni.

Questi attacchi possono avvenire solo se, in un modo od in un altro, i programmi vengono portati dentro il PC. I sistemi più comuni perchè ciò avvenga sono :

- navigando su siti internet;
- copiando dati da un supporto esterno (Cd_Rom, DVD, ...) non preventivamente ispezionato;

- aprendo file di MSWord ®, Excel ®, immagini, messaggi E_mail.

Per ridurre le possibilità di subire attacchi ogni PC è dotato di strumenti che controllano gli eventi e più precisamente:

- Firewall : Programma che controlla il traffico tra il PC ed il resto della rete (agisce in tempo reale).
- Anti virus : Programma che analizza i dati presenti sul disco e le istruzioni in esecuzione cercando istruzioni malefiche (agisce in tempo reale).
- Anti keylogger : Programmi che analizzano i dati sul disco cercando programmi appartenenti alle categorie spyware, keylog etc (non agisce in tempo reale).

Gli strumenti installati hanno la caratteristica di segnalare all'operatore ogni anomalia attraverso messaggi che compaiono sullo schermo a volte anche interrompendo i lavori in corso.
Ogni messaggio apparso deve essere immediatamente segnalato alla struttura delegata alla gestione del sistema informatico la quale provvederà a indicare come operare.

Disabilitazione programmi e/o procedure.

Per disabilitazione si intende la temporanea messa fuori utilizzo dei programmi e/o delle procedure che sono attive in modo automatico; molti di questi programmi e/o procedure sono importanti per la funzionalità del PC e/o della sua protezione.
È fatto divieto di disabilitare prodotti installati se non autorizzati dal Titolare.
È soprattutto vietato disabilitare anche solo temporaneamente i sistemi di difesa quali antivirus e firewall locali; tale atto per la gravità del rischio sarà immediatamente oggetto di azione disciplinare.

Creazione raccolte dati sui PC.

Sono riportate le linee guida che devono osservare tutti coloro che nell'ambito dei propri compiti effettuano in modo indipendente dal Sistema Centrale elaborazioni contenenti dati personali organizzati in archivi ordinati e/o ordinabili (fogli di calcolo, testi e/o data base).
Non rientrano nelle prescrizioni le raccolte di dati effettuate con dati anonimi. Si definiscono anonimi i dati che non possono essere ricondotti a persone fisiche, giuridiche, enti o associazioni in alcun modo, neanche indirettamente tramite codici ad esempio cliente/fornitore.
Per poter effettuare i trattamenti gli operatori devono :

- possedere l'incarico scritto a trattare i dati richiesti;
- stabilire per quanto tempo devono esistere i dati e come cancellarli dopo

averli utilizzati;

- recuperare solo le informazioni strettamente necessarie allo scopo limitando al massimo i riferimenti diretti alle persone giuridiche, fisiche enti o associazioni;
- custodire le informazioni in modo tale da impedire l'accesso a tutti coloro che non sono direttamente coinvolti nel processo;
- assicurarsi della correttezza delle informazioni, soprattutto quelle generate con istruzioni proprie;
- gestire la cancellazione dei dati una volta raggiunto lo scopo della raccolta.

Salvataggio e/o copia dati.

Ogni PC è dotato di spazio locale per poter contenere informazioni e ogni incaricato ha la possibilità di eseguire elaborazioni non centralizzate in modo autonomo come ad esempio effettuare indagini di comportamento economico dei clienti tramite fogli di calcolo, generare documenti interni o verso clienti/fornitori, gestire il piano di lavoro dei colleghi etc..
I dati generati vengono di norma conservati sul disco locale (C:) in directory a cura dell'incaricato il quale ne diventa l'unico responsabile ai fini della conservazione nel tempo e alla loro tutela impedendo l'uso difforme dai fini della raccolta.
La perdita anche involontaria dei dati o comunque la loro parziale o completa distruzione prima del termine di utilizzo può essere oggetto di gravi contestazioni verso l'incaricato ed in alcuni casi è possibile essere esposti a richieste di risarcimenti economici, oltre che essere una grave perdita di tempo e risorse.
Per salvaguardarsi da questo tipo di inconvenienti è utile, se non indispensabile, duplicare i dati su supporti diversi da quelli di normale uso (hard disk) e posti al riparo da facili attacchi tra i quali vanno compresi anche eventi naturali, danni fisici ai supporti, incendi ai locali, furti.
La tecnica metodologica usata per effettuare le azioni di salvaguardia si chiama *backup* ed è l'unica reale garanzia di salvaguardia dei dati; si tratta di duplicare le informazioni presenti nel PC su Cd_Rom, DVD o dischi removibili attraverso l'uso di particolari procedure.
Lo Studio ha messo a disposizione spazi disco sul server centrale il cui sistema di backup è gestito con regole di controllo e sotto la tutela del Titolare (o suo incaricato). L'incaricato dovrà effettuare la copia dei dati dal suo PC locale all'area del server centrale.
È comunque possibile effettuare dei backup localmente. L' uso di sistemi individuali di salvataggio, quali i Cd_Rom, DVD, chiavette USB, ..., deve avvenire in modo tale da impedire che i dati salvati possano, anche

involontariamente, essere diffusi o comunque portati all'esterno delle aree dello Studio senza esplicita autorizzazione.

Riservatezza /protezione documenti personali.

Nonostante l'accesso ai PC sia controllato da password può capitare che in determinate situazioni tale difesa possa essere insufficiente a garantire una corretta riservatezza delle informazioni; ad esempio in caso di furto del PC il ladro ha a disposizione più mezzi e tempo per forzare le sicurezze.

Nel caso lo Studio dovesse detenere informazioni di tipo sanitario, per i quali il G.D.P.R. richiede maggiori garanzie, lo Studio si doterà di programmi particolari che possono trasformare un archivio normale in un archivio criptato , ovvero illeggibile senza possedere la relativa chiave di interpretazione; attraverso l'uso di tali programmi gli archivi sono tutelati da trattamenti indesiderati con un livello di sicurezza a standard militare.

La protezione di documenti MSWord ® o Excel ® tramite l'utilizzo di password non è da considerarsi sicura perché facilmente violabile da programmi di grande diffusione.

Cancellazione dati e documenti.

Nonostante l'apparenza, tramite i comandi di cancellazione (messa nel cestino), presenti sui PC dotati di sistema operativo Microsoft Windows, i dati non vengono in realtà cancellati ma, per regole del sistema operativo medesimo, sono ancora disponibili per ulteriori usi.
La stessa funzione di cestino prevede l'opzione di recupero dei dati precedentemente posti nel cestino (opzione ripristino dati) se questo non è ancora stato eliminato; questo è un chiaro ed evidente indicatore del fatto che i dati in realtà non vengono cancellati ma solo segnalati come cancellati al Sistema Operativo rendendoli quindi disponibili per utilizzi fuori controllo.
Per realizzare la vera cancellazione, ovvero l'eliminazione sicura dei dati, è necessario utilizzare specifici programmi che oltre ad eliminare i dati riscrivono gli spazi precedentemente occupati dai dati eliminati con valori tali da impedire ogni possibilità di successivi tentativi di ricostruzione anche se effettuati con l'ausilio di particolari strumenti.
Il G.D.P.R. prevede l'obbligo, soprattutto se si tratta di dati *sensibili,* di cancellazione dei dati con strumenti tali che impediscano la possibilità di successive ricostruzioni, soprattutto se i dati da cancellare contengono informazioni di tipo sensibile.
Per la cancellazione dei dati si deve operare nel seguente modo:

- Cd / DVD (ogni tipo) : Distruzione fisica del supporto.

- Disco fisso : Esecuzione programma specifico di wiping.
- Disco rimovibile : Formattazione di basso livello / Esecuzione programma specifico di wiping.
- Chiavette USB: Esecuzione programma specifico di wiping.

Navigazione su internet.

Internet è una forma particolare di collegamento tra vari computer ed è strumento operativo indispensabile all'interno dello Studio; attraverso Internet è possibile avere alcune informazioni necessarie allo svolgimento del proprio compito, comunicare con clienti e/o fornitori e/o collaboratori via posta elettronica o altri sistemi di comunicazione, scambiare dati di notevole importanza per l'attività dello Studio.
L' accesso ad internet avviene tramite sistemi di connessione centralizzata e controllata; ogni attività su internet viene monitorata e registrata su particolari LOG ai fini di indagine per la ricerca di eventi delittuosi e dei relativi attori.
L' uso di Internet espone il PC e il suo utilizzatore a una serie di rischi alcuni dei quali possono comportare conseguenze estremamente gravi per l'incaricato; esiste anche la possibilità di essere involontariamente coinvolti in reati penali.
Per ridurre i rischi e salvaguardare l'incolumità degli incaricati sono stati messi in opera dei sistemi di difesa che però devono essere accompagnati da atteggiamenti comportamentali a carico degli incaricati medesimi.

I sistemi di difesa sono:

- browser affidabili;
- antivirus;
- ricercatori di spyware;
- firewall locali e centrali;
- sistemi di analisi del traffico su internet;
- sistemi di filtro per la navigazione su internet;

tali strumenti, come già detto, non sono sufficienti a tutelare da eventuali intrusioni, è sempre necessario che l'utente operi con la dovuta cautela e prudenza ogni qualvolta tratti con programmi destinati ad effettuare comunicazioni via rete.
Nello schema seguente sono indicate le azioni su internet che vanno assolutamente evitate:

- Utilizzare strumenti per la navigazione diversi da quelli autorizzati;
- Installare o concedere l'installazione di plug-in senza l'autorizzazione del Titolare;
- Interagire con siti che aprono finestre senza richiesta (pop up);
- Interagire con siti che contengono richiami (link) a siti pornografici,

pedofili, scarico musica, scambio archivi;
- Comunicare dati personali o aziendali su siti non conosciuti e certificati;
- Accedere a siti non conosciuti e comunque non attinenti allo scopo lavorativo;
- Iscriversi a liste di distribuzione;
- Partecipare a chat;
- Scaricare programmi o quant'altro dalla rete senza preventiva autorizzazione;
- Disabilitare gli strumenti di controllo e verifica dati presenti sul PC;
- Utilizzare programmi P2P (peer to peer) ovvero quei programmi che permettono la condivisione di archivi per scaricare film, musiche etc.

Gli incaricati sono tenuti a segnalare ogni evento o attività effettuata tra quelle sopra indicate al Titolare onde evitare le conseguenze già indicate.

Uso della posta elettronica e_mail.

È lo strumento per eccellenza di comunicazione tra vari soggetti che viene dato in concessione solo ed esclusivamente per scopi legati alle attività lavorative dello Studio; viene utilizzato sia per comunicazioni interne allo Studio, tra i vari appartenenti alle strutture, che esterne, tra lo Studio e i Clienti e/o i Fornitori.
Nonostante l'apparenza, la posta elettronica può essere utilizzata anche per trasmettere contenuti diversi dai messaggi di puro testo, ad esempio con gli allegati o messaggi in formato HTML è possibile trasmettere istruzioni, anche nascoste, eseguibili dal computer che riceve i messaggi.
Attualmente il miglior modo di diffondere virus informatici è la posta elettronica.
Secondo la normativa vigente i messaggi di posta possono anche essere mezzo per perpetrare reati informatici ad esempio partecipando a catene di Sant'Antonio.
Esistono due tipologie di comportamento da tenere nei confronti della posta elettronica:
- quando si ricevono messaggi;
- quando si inviano messaggi;

Comportamenti quando si ricevono messaggi.

La ricezione di un' e_mail espone potenzialmente il PC alla ricezione di virus e comunque di programmi *malefici.*
Per ridurre questo rischio è innanzi tutto necessario che il sistema antivirus sia attivo, aggiornato ed abilitato ad analizzare gli allegati in tempo reale.
Ma le difese tecniche possono essere superate da cattivi comportamenti, ed è

quello su cui si basano nuove metodologie di contagio.
E' necessario, quindi, che l' incaricato adotti particolari comportamenti che si riassumono in:

- non aprire allegati se non si è sicuri della provenienza di un messaggio;
- non seguire i link presenti nel messaggio se non si è sicuri della provenienza;
- non attivare l'esecuzione automatica degli allegati;
- disabilitare la visualizzazione delle immagini e richiederla in modo esplicito solo nei messaggi di provenienza sicura;
- disabilitare l'anteprima dei messaggi.

Comportamenti quando si inviano messaggi e_mail.

L'invio di un messaggio di e_mail nasconde alcune insidie che possono rilevarsi fastidiose sia per il destinatario che per il mittente. (quest'ultimo rischia anche problemi legali).
La legge punisce chiunque diffonda con ogni mezzo programmi atti a danneggiare o impedire l'uso di sistemi informatici. Viene punito l'atto doloso oltre che l'atto volontario ed è prevista la reclusione.
Per ridurre tali rischi è necessario comportarsi secondo le seguenti regole:

- non disabilitare il controllo antivirus per i messaggi in uscita;
- non partecipare a catene di Sant'Antonio ovvero non accettare di ritrasmettere messaggi ad altri destinatari;
- non indicare gli indirizzi di tutti i corrispondenti in caso di invii multipli ma inviare singoli messaggi o richiedere l'attivazione di funzioni di mailing list al Titolare;
- non 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;
- non utilizzare programmi di dialogo quali chat e/o messaggistica MSN Messenger o similari, anche definiti via WEB;

In base alla normativa vigente, ai fini di tutelare lo Studio e l'operato dei propri collaboratori, lo Studio ha diritto di controllare attraverso strumenti automatici e/o azioni dirette il contenuto delle e-mail con il fine ultimo di individuare azioni e/o contenuti pericolosi all'attività dello Studio e dei propri collaboratori.

TRATTAMENTI MANUALI

Regola generale.

I trattamenti manuali sono fortemente presenti presso ogni struttura aziendale.
Per trattamento manuale si intende ogni trattamento che viene effettuato senza l'ausilio di strumenti informatici, sono quindi trattamenti manuali tutti gli scritti presenti presso le strutture dell'ufficio oltre alle pure informazioni verbali delle quali si viene a conoscenza.
I trattamenti manuali sono sottoposti a pericoli diversi rispetto ai trattamenti informatici, uno dei più subdoli è la diffusione dell'informazione.
Come indicato nel testo del G.D.P.R. e già detto precedentemente, per diffusione si intende anche il mettere a disposizione i dati; lasciare uno scritto sulla scrivania senza controllo diretto corrisponde ad un atto di diffusione, come il gettare nel cestino della carta straccia documenti contenenti informazioni personali senza prima averli resi anonimi o comunque resi illeggibili.
Vengono indicati alcuni comportamenti da tenersi :

- alla fine della giornata assicurarsi che la scrivania sia sgombera da documenti e ogni altra informazione che possa ledere i diritti degli interessati;
- la documentazione cartacea non più usata deve essere eliminata tramite l'apposito distruggi carta;
- tenere chiusi armadi contenenti documenti;
- rendere anonimi i dossier;
- astenersi dai commenti che coinvolgano terze persona