STUDIO LEGALE
SALARDI
International Law & Business

Atto di nomina dell'Incaricato del trattamento dei dati personali, ai sensi e per gli effetti dell'art. 30 del D. Lgs. 30 giugno 2003 n. 196

Sig.ra Monica Riva

In base a quanto previsto dall'art. 30 del decreto legislativo 30 giugno 2003, n.196 ed in osservanza del Codice Deontologico Privacy (Provvedimento del Garante n. 60 del 06.11.2008, pubblicato nella G.U. n. 275 del 24.11.2008) sulla tutela del trattamento dei dati personali, la Sig.ra Monica Riva, nella Sua qualità di incaricato del trattamento dei dati personali, ha accesso alle banche dati dello Studio Legale Salardi, con sede in Modena, Via Cesare Costa 19/D.
In particolare, in osservanza dei suddetti impegni, Lei, in qualità di collaboratore dello Studio Legale Salardi ed incaricato del trattamento dovrà prestare le seguenti attività:

collaborazione, praticantato e formazione della attività forense in generale;

Ai fini di una corretta applicazione della legge citata, nonché di una adeguata tutela dei diritti degli Interessati, Lei dovrà:

- svolgere operazioni di trattamento unicamente sui dati sui quali si è autorizzati all'accesso, nel corretto svolgimento dei compiti cui si è preposti;
- astenersi dal comunicare i dati personali a soggetti diversi da quelli indicati dallo Studio legale o che non abbiano motivo di acquisire tali dati per il corretto espletamento dei propri compiti;
- custodire e controllare i documenti contenenti dati personali utilizzati per l'esercizio delle proprie attività in modo da evitare l'accesso a soggetti estranei;
- mantenere i dati in modo tale che siano esatti, completi, veritieri;
- correggere o segnalare eventuali dati inesatti;
- restituire integralmente allo Studio Legale i dati personali in Suo possesso o custodia e che a seguito della cessazione o modifica delle mansioni svolte, non si ha più ragione di utilizzare, con espresso divieto di conservarli in copia, duplicarli, comunicarli o diffonderli;
- segnalare al firmatario della presente il verificarsi di qualsiasi evento inaspettato che riguardi l'integrità, la riservatezza o la disponibilità delle informazioni.
- rilasciare – a fine lavori - una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni dell'Allegato B - D.Lgs. 196/2003 (Codice in Materia di Protezione dei Dati Personali);
- osservare con la massima diligenza le regole indicate nel Disciplinare in Materia di Utilizzo degli Strumenti Informatici in osservanza del Provvedimento Generale del garante del 1 marzo 2007, **Allegato 1** al presente atto di nomina e pubblicato sul sito dello Studio Legale Salardi.
- Osservare con la massima diligenza le Istruzioni per l'Incaricato di cui all'**Allegato 2** al presente atto.

Oltre alle sopracitate istruzioni – in linea generale - gli Incaricati del trattamento debbono rispettare la massima riservatezza e discrezione nella gestione dei dati e relativi supporti, ponendo in essere, relativamente ai soli dati a cui l'Incaricato accede in relazione all'intervento rientrante nella specifica tipologia di cui sopra, ogni attività necessaria ad evitare i rischi di perdita o distruzione - anche accidentale - dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità per cui i dati furono raccolti.

Le presenti istruzioni – e le future che dovessero essere formalmente comunicate - sono impartite in ottemperanza di precisi obblighi di legge ed integrano le norme inerenti lo svolgimento dei compiti affidati: pertanto ciascun Incaricato è impegnato ad un preciso rispetto delle stesse.

La presente nomina avrà la medesima durata del servizio espletato presso lo Studio Legale e cesserà automaticamente alla cessazione, per qualsiasi motivo, dello stesso. Sarà comunque diritto del Titolare revocarla in qualsiasi momento.

Modena, lì 02.01.2016

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

Per ricevuta e integrale accettazione.

Firma dell'Incaricato 

Monica Riva

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

Allegato 1

Lavoro: le linee guida del Garante per posta elettronica e internet
Gazzetta Ufficiale n. 58 del 10 marzo 2007

Registro delle deliberazioni
Del. n. 13 del 1° marzo 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici;

Vista la documentazione in atti;

Visti gli artt. 24 e 154, comma 1, lett. b) e c) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

PREMESSO

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. Premessa
Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Occorre muovere da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);
c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili. (1)

1.2. Tutela del lavoratore
Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. (2)

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato). (3)

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. Principi generali
Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del Codice). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. Discipline di settore
Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (art. 47, comma 3, lett. b) Codice dell'amministrazione digitale). (4)

2.3. Principi del Codice
I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2);
b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. par. 3);
c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice: par. 4 e 5), osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001, cit., punti 5 e 12).

3. Controlli e correttezza nel trattamento

3.1. Disciplina interna
In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, secondo comma, Statuto dei lavoratori;allegato VII, par. 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all'insaputa dei lavoratori"). (5)

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. Linee guida
In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il download di software o di file musicali), oppure alla tenuta di file nella rete interna;
in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime –specifiche e non generiche– per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
PIVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

3.3. Informativa (art. 13 del Codice)
All'onere del datore di lavoro di prefigurare e pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2..

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art. 4, secondo comma, l. n. 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.).

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli. (6)

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori. É il caso, ad esempio:

della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
dell'analisi occulta di computer portatili affidati in uso.
Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. (7) A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice). (8)

5. Programmi che consentono controlli "indiretti"

5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. (9) Ciò, anche in presenza di attività di controllo discontinue. (10)

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati (11), nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. (12)

5.2. Principio di necessità
In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori (artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4).

Dal punto di vista organizzativo è quindi opportuno che:

si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet; (13)
si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.
Il datore di lavoro ha inoltre l'onere di adottare tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (c.d. privacy enhancing technologies–PETs). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

a) Internet: la navigazione web
Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni –reputate inconferenti con l'attività lavorativa– quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.
b) Posta elettronica
Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i file allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale). (14)

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita").

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; (15)
il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. (16) In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

6. Pertinenza e non eccedenza

6.1. Graduazione dei controlli

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. Conservazione
I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla (v. art. 11, comma 1, lett. e), del Codice).

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.
In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. Datori di lavoro privati
I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (v., in particolare, art. 4, secondo comma, dello Statuto), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.

Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (art. 24, comma 1, lett. f) del Codice);
b) in caso di valida manifestazione di un libero consenso;
c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice).

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. Datori di lavoro pubblici
Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (artt. 18-22 e 112).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. a), del Codice).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (art. 29 del Codice).

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9).

TUTTO CIÒ PREMESSO IL GARANTE

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:

a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);

b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:

si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;
c) l'adozione di misure di tipo tecnologico, e segnatamente:

I. rispetto alla "navigazione" in Internet (punto 5.2., a):

l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
la graduazione dei controlli (punto 6.1.);
II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):

la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;

b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

d) l'analisi occulta di computer portatili affidati in uso;

4) individua, ai sensi dell'art. 24, comma 1, lett. g), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
PIVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

5) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 1° marzo 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

Allegato 2

Istruzioni per l'Incaricato

La legge definisce come incaricati "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".
Limitatamente all'ambito di competenza a lei assegnato nella Nomina dal Titolare o dal Responsabile, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alle normative vigenti sulla Privacy.

REGOLE OPERATIVE

1. PROCEDURE PER LA CLASSIFICAZIONE DEI DATI.

L'incaricato deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge.
La natura dei dati trattati
La Legge definisce "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Vengono riportate di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:

- dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;
- dati sensibili: la lettera d) del comma 1 dell'articolo 4 del codice definisce in tale modo i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
- dati giudiziari: tali sono considerati, dalla lettera e) del comma 1 dell'articolo 4 del codice, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u) del Dpr 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- dati che presentano rischi specifici: tali dati sono considerati dall'articolo 17. Si tratta di dati che, pur non essendo così delicati come quelli sensibili e giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati, ovvero alle modalità di trattamento o agli effetti che esso può determinare: in considerazione di tale fatto, il loro trattamento è ammesso nel rispetto delle misure e degli accorgimenti, prescritti dal Garante a garanzia dei soggetti interessati.

2. AFFIDAMENTO AGLI INCARICATI DI DOCUMENTI, CONTENENTI DATI PERSONALI, E MODALITÀ DA OSSERVARE PER LA CUSTODIA DEGLI STESSI.

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI
Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare o del Responsabile in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni.
Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre provvedere in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni affidate.

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
PIVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

In caso di affidamento di atti e documenti contenenti dati sensibili o giudiziari, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa). In mancanza di tali strumenti sollecitare la Direzione affinché provveda.
Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.
Qualora si debbano utilizzare anche nei giorni successivi i documenti potranno essere riposti in tali cassetti al termine della giornata di lavoro. Al termine del trattamento dovranno invece essere restituiti all'archivio.

3. MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD, NONCHÉ PER FORNIRNE UNA COPIA AL PREPOSTO ALLA CUSTODIA DELLE PAROLE CHIAVE.

TRATTAMENTO CON L'AUSILIO DI STRUMENTI ELETTRONICI
Utilizzare sempre le credenziali di autenticazione (user ID e Password) fornite dall'Amministratore di Sistema o dal responsabile dell'area sicurezza.
Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.
Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.
Elaborare le password seguendo le istruzioni sotto riportate
Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Incaricato.

SCELTA DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

- NON dica a nessuno la sua password. Ricordi che lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.
- NON scriva la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
- Quando immette la password NON faccia sbirciare a nessuno quello che sta battendo sulla tastiera.
- NON scelga password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- NON creda che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- NON usi il suo nome utente. È la password più semplice da indovinare
- NON usi password che possano in qualche modo essere legate a lei come, ad esempio, il suo nome, quello di sua moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.
- Prestare attenzione quando si accede ai dati mediante strumenti occasionali o non aziendali

COSA FARE

- la password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è' buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica
- L'incaricato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema
- la password deve essere modificata dall'incaricato almeno ogni 6 mesi;

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

• se il trattamento riguarda dati sensibili o giudiziari la password deve essere modificata almeno ogni tre mesi ;
• Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi la password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema. In caso di dubbio, consultate il vostro amministratore di sistema.

4. OBBLIGO DI NON LASCIARE INCUSTODITI E ACCESSIBILI GLI STRUMENTI ELETTRONICI, MENTRE È IN CORSO UNA SESSIONE DI LAVORO.

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tipo il blocco della sessione, per cui anche in quei cinque minuti il computer non resti:
• incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
• accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.
Non si devono invece mai verificare situazioni in cui lo strumento elettronico viene lasciato attivo, durante una sessione di trattamento, senza che la stanza in cui è ubicato venga chiusa, né vi sia nei paraggi almeno una persona di fiducia.
È necessario:
• predisporre una copia della parola chiave, provvedendo quindi a trascriverla, facendo però in modo che l'informazione resti segreta (ad esempio, inserendola in una busta chiusa datata, firmata e sigillata)
• consegnare tale copia ad un soggetto, che sia stato previamente incaricato della sua custodia (l'incaricato per la custodia delle copie credenziali o parole chiave)

5. PROCEDURE E MODALITÀ DI UTILIZZO DEGLI STRUMENTI E DEI PROGRAMMI ATTI A PROTEGGERE I SISTEMI INFORMATIVI.

Verificare che il proprio antivirus sia aggiornato a non più di una settimana (7 giorni). Nel caso di portatile e di permanenza prolungata all'esterno dell'azienda provvedere all'aggiornamento manualmente come indicato dal Responsabile della sicurezza.
Installare le Patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale che diviene semestrale in caso di trattamenti di dai sensibili o giudiziari. In caso di aggiornamenti importanti riceverete un avviso dai Sistemi Informativi con le istruzioni operative che dovrete applicare come possibile

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido o a catturare informazioni riservate (password/chiavi di sblocco etc.)

FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

• riutilizzo di dischetti già adoperati in precedenza;
• uso di software gratuito (o shareware) prelevato da siti Internet o in allegato a riviste o libri;
• uso di dischetti preformattati;
• collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido;
• collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del server;
• uso di modem per la posta elettronica e prelievo di file da BBS o da servizi commerciali in linea o da banche dati;

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362
Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it
studiosalardi.it

- uso di modem mentre si è connessi alla intranet aziendale protetta
- ricezione di applicazioni e dati dall'esterno, Amministrazioni, fornitori, ecc.;
- utilizzo dello stesso computer da parte di più persone;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
- file attached di posta elettronica.

COME PREVENIRE I VIRUS:

1. USI SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato ed autorizzato. Non utilizzi programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. SI ASSICURI DI NON FAR PARTIRE ACCIDENTALMENTE IL SUO COMPUTER DA DISCHETTO

Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files. Normalmente l'antivirus effettua questo controllo quando si spegne il computer ed evidenzia lo stato mediante una segnalazione

3. PROTEGGA I SUOI I DISCHETTI DA SCRITTURA QUANDO POSSIBILE

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

- Non si deve utilizzare il proprio "disco sistema" su di un altro computer se non in condizione di "protezione in scrittura".
- Se si utilizza un computer che necessita di un "bootstrap" da floppy, usare un floppy disk protetto in scrittura.
- Non attivare mai da floppy un sistema basato su hard disk a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto;

4. SI ASSICURI CHE IL SUO SOFTWARE ANTIVIRUS SIA AGGIORNATO

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Si informi attraverso il Portale della privacy sugli obblighi di legge in tema di aggiornamento degli antivirus e applichi, se possibile, una frequenza di aggiornamento mensile (più idonea di quella prevista dalla legge).

5. NON DIFFONDA MESSAGGI DI PROVENIENZA DUBBIA

Se riceve messaggi che avvisano di un nuovo virus pericolosissimo, lo ignori: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete.

Questo è vero anche se il messaggio proviene dal suo migliore amico, dal suo capo o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

6. NON PARTECIPI A "CATENE DI S. ANTONIO" E SIMILI

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

7. LIMITI LA TRASMISSIONE DI FILE ESEGUIBILI (.COM, .EXE, .OVL, .OVR) E DI SISTEMA (.SYS) TRA COMPUTER IN RETE

8. NON UTILIZZI I SERVER DI RETE COME STAZIONI DI LAVORO

9. NON AGGIUNGA MAI DATI O FILE AI FLOPPY DISK CONTENENTI PROGRAMMI ORIGINALI

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

10. NON CONDIVIDA NESSUNA CARTELLA DEL SUO COMPUTER MA UTILIZZI I FILE SERVER O SERVER FTP

6. PROCEDURE PER IL SALVATAGGIO DEI DATI.

Gli incaricati sono tenuti a fare riferimento alla politica di back up dell'azienda per le istruzioni specifiche di salvataggio. Se è nominato l'incaricato delle copie di back up, egli sarà il referente per tali operazioni.

7. CUSTODIA ED UTILIZZO DEI SUPPORTI RIMUOVIBILI, CONTENENTI DATI PERSONALI.

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. dischetti, CD), contenenti dati sensibili o giudiziari, nei seguenti termini:
• I supporti rimovibili (es. dischetti), contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
• Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

8. DOVERE DI AGGIORNARSI, UTILIZZANDO IL MATERIALE E GLI STRUMENTI FORNITI DALL'ORGANIZZAZIONE, SULLE MISURE DI SICUREZZA.

Pretendere dal titolare che vengano forniti strumenti per la formazione sulla privacy. In particolare relativamente a:
• profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano
• misure disponibili per prevenire eventi dannosi
• modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

ISTRUZIONI GENERICHE

L'INCARICATO DOVRA':
procedere alla raccolta di dati personali, nelle modalità previste dalle sue mansioni e indicate in apposita informativa;
consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa di cui all'art. 13 del nuovo Codice della Privacy, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;
raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il Titolare o il Responsabile, e salvo i casi di esonero previsti dalla stessa legge;
trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;
adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate dal Titolare o dal Responsabile, in particolare dovrà:
• per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
PIVA 03049660362
Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it
studiosalardi.it

anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
• trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
• conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
• con specifico riferimento agli atti e ai documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
• utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
• copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento, copie di dati sensibili devono essere espressamente autorizzate dal Responsabile del trattamento o dal Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
• in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento o al Titolare; segnalare al Titolare o al Responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal Titolare o dal Responsabile e secondo le modalità stabilite dai medesimi e dichiarate nell'informativa;
mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
in generale, prestare la più ampia e completa collaborazione al Titolare ed al Responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Manutenzione e gestione dei sistemi di elaborazione elettronica.

Tale area di competenza riguarda tutte le operazioni inerenti alla gestione e alla manutenzione del sistema informatico. Nel momento in cui i dati personali vengono trattati con l'ausilio di strumentazione informatica, la loro gestione deve essere conforme alle disposizioni di Legge in materia di sicurezza dei dati, come prescritto nel Codice della Privacy. In particolare Lei è tenuto a:
• Installare su tutte le postazioni client, sui server, sui PC e dove necessario (limitatamente all'ambito di competenza a lei assegnato) gli antivirus e aggiornarli con cadenza almeno semestrale! Si consiglia una frequenza del tutto più restrittiva.
• Effettuare tutti gli aggiornamenti patch dei sistemi operativi e dei programmi utilizzati per il trattamento dati, con cadenza annuale che diviene semestrale in caso di trattamenti di dai sensibili o giudiziari;
• Definire le politiche di protezione passiva della rete (firewall e sua configurazione) per la difesa del sistema dall'attacco di hackers;
• Verificare l'efficacia delle politiche di sicurezza almeno con cadenza semestrale;
• Collaborare con gli altri responsabili mantenendoli informati della gestione e di eventuali anomalie di sistema che potrebbero compromettere la sicurezza;
• Istruire gli incaricati dei back-up riguardo alle procedure da adottare per le operazione di salvataggio delle copie di sicurezza dei dati personali, redigendo apposito documento di istruzioni. Risolvere gli eventuali problemi tecnici nella realizzazione dei back-up rilevati dai rispettivi incaricati.

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

• Sottoscrivere il documento con le istruzioni per il back up, conservarlo in luogo sicuro e trasmetterlo in copia agli incaricati del trattamento dei dati interessati alle copie di salvataggio, nonché all'incaricato dei back up di quella base dati.
Per ogni base dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up e le modalità di custodia.
• Nel caso in cui la manutenzione venisse affidata ad una società esterna, è opportuno ricevere dalla stessa i nominativi delle persone che provvederanno alla manutenzione, al fine di redigere una lettera di incarico delle stesse; per tali operazioni fare riferimento al Titolare o al Responsabile dei trattamenti.

Back Up dei dati

Per back up si intende l'insieme di operazioni e di procedure mirate ad effettuare una copia di sicurezza dei dati personali memorizzati su dispositivi informatici, in modo da rendere possibile un eventuale ripristino dei dati nel caso si verifichino eventi dannosi che portino al danneggiamento od alla perdita (totale o parziale) dei dati personali. In quanto incaricato della realizzazione dei Back-up in relazione alle banche dati di sua competenza, Lei è tenuto ad :
• Effettuare una copia dei dati personali almeno una volta alla settimana.
• Collaborare con l'Amministratore di Sistema o con il Responsabile dell'area sicurezza per la sequenza delle operazioni tecniche da effettuare.
• Segnalare in modo sollecito al relativo Responsabile o all'Amministratore di Sistema il presentarsi di eventuali problemi alla normale attività di copia delle basi di dati.
• Le copie di back-up devono essere custodite ed utilizzate in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
• Particolare attenzione va riservata alle copie di back-up contenenti dati sensibili o giudiziari: è bene conservare gli archivi di back-up in cassetti chiusi a chiave, durante il periodo di conservazione, e successivamente formattarli quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
• Nel caso di perdita di dati sensibili o giudiziari il ripristino delle copie di back-up deve essere effettuato in modo da consentire la ripresa a pieno regime entro e non oltre una settimana di tempo. A tale scopo, l'incaricato deve rifarsi al piano di continuità elaborato dal titolare o dal responsabile al trattamento.
• Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

Custodia delle Copie Credenziali

Il Codice della Privacy impone che siano studiate ed applicate procedure per consentire la continuità operativa dei trattamenti anche nel caso in cui un incaricato rimanesse a lungo assente o dimenticasse la propria password. A tale scopo una modalità comunemente adottata è quella di nominare un CUSTODE DELLE COPIE CREDENZIALI.
In tal caso Lei è tenuto a:
• Assicurarsi di avere in custodia tutte le copie delle parole chiave degli incaricati della propria azienda.
• Conservare le copie delle parole chiave chiuse in una busta munita di sigillo apposto direttamente dall'incaricato proprietario della parola stessa.
• Conservare tali buste in contenitore chiudibile a chiave ed assicurarsi di essere l'unico custode dell'accesso a tale contenitore. Anche il Titolare non deve accedervi se non previa Sua autorizzazione e per giustificato motivo. Deve sempre essere possibile risalire a chi ha aperto una busta ed ha utilizzato la parola chiave per un accesso.
• In caso di assenza di un incaricato e di necessità ad operare un trattamento in sua vece, autorizzare l'apertura della busta e assegnare l'operatività ad altro incaricato; effettuare immediata comunicazione all'interessato assente di quanto

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it

accaduto. Al suo ritorno ripristinare l'operatività originaria dopo che l'incaricato ha rieditato una nuova password e consegnato una copia.

Sorveglianza degli Archivi ad Accesso Controllato

Tale area di competenza riguarda le operazioni di sorveglianza e controllo degli archivi contenenti dati sensibili o giudiziari. In particolare Lei è tenuto a:

- Assicurarsi che tali archivi siano situati in contenitori od uffici chiudibili a chiave.
- Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.
- Nel caso non vi siano apparecchiature elettroniche che identifichino e registrino gli accessi all'archivio od all'ufficio, tenere un registro manuale degli accessi fuori orario di lavoro. I soggetti che vengono ammessi agli archivi, dopo l'orario di chiusura degli stessi, devono essere identificati e registrati.

Studio Legale Salardi
Associazione Professionale
Via Cesare Costa 19/D
41123 Modena, Italy
P.IVA 03049660362

Tel +39 059 332676
Fax +39 059 822023
info@studiosalardi.it

studiosalardi.it