Afol Monza e Brianza

Tre Venezie, 63
20821 Meda (MB)
Tel: 3346242996
P.IVA 06413980969

ISTRUZIONI PER L'ADDETTO

L'Art.29 Reg. UE 2016/679 definisce come addetti "le persone fisiche che sotto la responsabilità di un Titolare o di un Responsabile agiscono accedendo a dati personali".

Nell'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.

PROCEDURE PER LA CLASSIFICAZIONE DEI DATI.

L'Addetto deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge. Qualora non fosse in grado, deve fare riferimento al Responsabile o al Titolare del Trattamento.

La natura dei dati trattati

Vengono riportate di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:

- «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 genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- «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;

AFFIDAMENTO AGLI ADDETTI 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.

In caso di affidamento di atti e documenti contenenti dati di categorie particolari, 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 contenenti 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.

I SISTEMI INFORMATICI AZIENDALI

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto: tali strumenti vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità aziendali. In questo contesto l'azienda potrà per necessità di sicurezza aziendale o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

Utilizzo del personal computer

- é consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Titolare o dal Responsabile; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici; non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);
- non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
- i Personal Computer "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Utilizzo di internet

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
- non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo relativa a dati 'particolari' ai sensi del Reg. UE 2016/679: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare o dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dal Titolare o dal Responsabile;
- non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa la partecipazione durante l'orario di lavoro, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Utilizzo del servizio di posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività aziendale;
- nel caso esista un dominio di proprietà aziendale (es.: nomeazienda.it) al quale sia collegato un servizio di posta e la relativa casella (es.: rossi@nomeazienda.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai dominii aziendali salvo diversa ed esplicita autorizzazione.

MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD

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.

Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Addetto.

Nel caso in cui sia prevista la figura del custode delle copie credenziali, è necessario trascrivere una copia della propria parola chiave e consegnarla in busta chiusa (meglio se sigillata) all'Addetto od al responsabile incaricato alla loro custodia. Fare riferimento al Titolare od al Responsabile per i dettagli operativi della procedura.

Elaborare le password seguendo le istruzioni sotto riportate.

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 usa una password è assicurare che nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.
- NON scriva la password in nessun posto in cui 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.

COSA FARE OBBLIGATORIAMENTE

- 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'Addetto 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'Addetto almeno ogni 6 mesi;
- se il trattamento riguarda dati sensibili o giudiziari la password deve essere modificata almeno ogni tre mesi ;

COSA FARE PRATICAMENTE

Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.

Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un ottima protezione contro possibili violazioni. Non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri: ad esempio i sistemi operativi Windows 95 98 e Me non oltrepassano questo limite.

Utilizzare numeri e simboli al posto di caratteri

Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:

- Caratteri minuscoli: a, b, c,...
- Caratteri maiuscoli: A, B, C,...
- Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
- Caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?

Non inserirli alla fine di una parola nota come ad es.:"computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3"al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista.

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 tali, 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 venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un Addetto al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.

E' possibile installare strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previa imputazione di password. Verifichi con i Responsabili o con il Titolare le possibilità di abilitazione dello strumento.

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

In collaborazione con i Responsabili o con il Titolare, che possono installare dove previsti degli automatismi in grado di sostituirsi all'Addetto, prevedere di:

- aggiornare con cadenza almeno mensile gli antivirus installati sulla propria postazione PC. Si consigliano ovviamente cadenza più serrate;
- 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 dati di categoria particolare.

FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

- riutilizzo di dischetti già adoperati in precedenza;
- uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri;
- 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.

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.

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. Non utilizzi programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. 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. Mantenga costantemente aggiornati i sistemi di protezione in accordo con le policy di sicurezza e comportamento aziendali.

3. Si assicuri che il suo PC sia stato controllato dall'antivirus

Almeno una volta alla settimana e provveda a lanciare una scansione dell'intero sistema con il suo software antivirus. Se questo software lo prevede, scheduli anche in questo caso la programmazione della scansione in maniera tale da non doversi ricordare di lanciarla e lasciando che il programma la esegua in automatico. Si consulti con i Responsabili o con il Titolare per le informazioni necessarie.

4. 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).

5. Non partecipi a "catene di S. Antonio" o 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.

6. Eviti la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete

7. Non utilizzi i server di rete come stazioni di lavoro

8. Non aggiunga mai dati o file a memorie di massa removibili a meno che non siano proteggibili in scrittura e con sistema di accesso controllato;

9. 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.

10. Protegga i suoi 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 memorie di massa contenenti Dati Personali su altro computer se non in condizioni di protezione in scrittura;
- Se si utilizza un computer che necessita di essere avviato tramite memoria di massa rimovibile, assicurarsi che non contenga dati personali;
- Verificare all'inserimento su computer di Memorie di massa rimovibili l'eventuale presenza di Virus e Malaware con Verifica Automatica o manuale;

OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI

Anche informazioni di normale quotidianità aziendale o ritenute non riservate all'interno dell'interscambio tra Addetti, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un

requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

SOCIAL ENGINEERING

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

E-MAIL PHISHING

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Spesso queste tecniche sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima

COSA FARE

- non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- limitatevi a fornire informazioni a interlocutori noti e operanti con voi per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato;
- diffidate di messaggi provenienti da fonte non conosciuta;
- non aprite messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprite messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il Responsabile o il Titolare.

PROCEDURE PER IL SALVATAGGIO DEI DATI.

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

CUSTODIA ED UTILIZZO DEI SUPPORTI RIMUOVIBILI, CONTENENTI DATI PERSONALI.

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. dischetti), 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.

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;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

ISTRUZIONI GENERICHE

L'ADDETTO DOVRÀ:

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 agli artt. 13-14 del Reg.to UE 2016/679, 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 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 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 rimuovibili 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:

- Assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda.
- Definire le politiche di protezione dei sistemi verso l'attacco di programmi (Virus) per tutte le basi dati elettroniche;
- 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 dati 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.
- Sottoscrivere il documento con le istruzioni per il back up, conservarlo in luogo sicuro e trasmetterlo in copia agli Addetti del trattamento dei dati interessati alle copie di salvataggio, nonché all'Addetto 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.
- Predisporre (nella sua qualità di "Amministratore di Sistema") sistemi idonei alla registrazione degli accessi logistici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

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 Addetto 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'Addetto 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 196/2003 imponeva che fossero studiate ed applicate procedure per consentire la continuità operativa dei trattamenti e quindi l'accesso ai computer anche nel caso in cui l'Addetto rimanesse a lungo assente o dimenticasse la propria password. Nell'ipotesi che i sistemi in uso non fossero in grado di permettere l'accesso di un altro soggetto con privilegi superiori (quello che in gergo tecnico viene chiamato "Admin", "Administrator" o "Amministratore") in grado di azzerare la precedente password per assegnarne una nuova e rendere disponibile nuovamente all'uso la postazione, una modalità comunemente adottata è quella di nominare un CUSTODE DELLE COPIE CREDENZIALI che conserva in un luogo sicuro e in busta chiusa copia di tutte le password in uso, per consultarle nel momento in cui si rendesse necessario accedere ad un elaboratore privo dell'Addetto o nel caso questi avesse smarrito la password.

In questi casi, è necessario:

- predisporre una copia della parola chiave, provvedendo quindi a trascriverla in copia, facendo però in modo che l'informazione resti segreta (ad esempio, inserendola in una busta chiusa e, possibilmente, sigillata);
- consegnare tale copia all'Addetto per la custodia delle copie credenziali o parole chiave;
- ripetere i due punti precedenti per ogni sostituzione periodica.

Verificare nell'Organigramma Privacy la presenza della figura del CUSTODE DELLE COPIE CREDENZIALI.

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.