ISTRUZIONI OPERATIVE AGLI ADDETTI AL TRATTAMENTO DEI DATI

E

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS E PER LA SCELTA DELLE PASSWOD

C.I.A.P.I. (REGIONE SICILIANA)

Ex S.S 114, SNC

96010 PRIOLO GARGALLO (SR)

C.F: 80001330895

Di seguito si riportano le misure di sicurezza idonee da adottare a cura del Responsabile e degli Addetti, in caso di trattamento di dati personali senza l'ausilio di strumenti elettronici.

Modalità tecniche da adottare a cura del titolare, del responsabile e dell'addetto, in caso di trattamento con strumenti diversi da quelli elettronici:

- agli Addetti sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli addetti, la lista degli addetti può essere redatta anche per classi omogenee di mansione e dei relativi profili di autorizzazione;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli addetti del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- quando gli atti e i documenti contenenti dati personali, sensibili o giudiziari sono affidati agli addetti del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli addetti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Nell'ambito informatico il termine "sicurezza" si riferisce a tre aspetti distinti:

- **Riservatezza:** prevenzione contro l'accesso non autorizzato alle informazioni.
- **Integrità:** le informazioni non devono essere alterabili da incidenti o abusi.
- **Disponibilità:** il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi, misure soltanto tecniche, per quanto possono essere sofisticate non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessun strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

- **Utilizzare le chiavi:** il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario, non banale, per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponete i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.

- **Conservate i documenti in luoghi sicuri:** tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo, ma mai con i nominativi di clienti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno, se poste in luoghi controllati, o armadi con serratura o ripostigli con porte con serratura se posti in luoghi noti controllati o aperti al pubblico. I dati per cui viene richiesto il blocco o la cancellazione, ma che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno essere posti in armadi con serratura o ripostigli con porte con serratura. I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi

sicuri (locali in muratura con porta blindata). Non lasciare documenti con dati personali sui tavoli, dopo averli utilizzati, riponeteli sempre nei loro contenitori.

Istruzioni agli addetti al trattamento che trattano dati con strumenti elettronici

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

1. **Riservatezza**: Prevenzione contro l'accesso non autorizzato alle informazioni
2. **Integrità:** Le informazioni non devono essere alterabili da incidenti o abusi
3. **Disponibilità:** Il sistema deve essere protetto da interruzioni impreviste

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi, misure soltanto tecniche, per quanto possono essere sofisticate, non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

- **Utilizzare le chiavi:** il primo livello dì protezione di qualunque sistema è quello fisico: è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario, non banale, per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponete i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.

- **Conservare i documenti in luoghi sicuri:** tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo ma mai i nominativi di clienti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno; se poste in luoghi controllati, o in armadi con serratura o ripostigli con porte con serratura se posti in luoghi non controllati o aperti al pubblico. I dati per cui viene richiesto il blocco o la cancellazione, che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno essere posti in armadi con serratura o ripostigli con porte con serratura. I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione. I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi sicuri (locali in muratura con porta blindata). Non lasciare documenti con dati personali sui tavoli, dopo averli utilizzati; riponeteli sempre nei loro contenitori.

- **Conservare i CD/DVD in un luogo sicuro:** per i CD, DVD, dischetti, Pen-drive e per qualsiasi altro supporto removibile di dati, si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può essere anche dovuto a un furto) può passare più facilmente inosservato. Riponeteli quindi sotto chiave in armadi o archivi non appena avete finito di usarli.

- **Utilizzate le password:** vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
  i. la password di accesso al computer che impedisce l'utilizzo improprio della vostra postazione quando per un motivo qualsiasi non vi trovate in ufficio;
  ii. la password di accesso alla rete che impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'ufficio;
  iii. la password di programmi specifici che impedisce l'accesso ai documenti realizzati con quelle applicazioni;
  iv. la password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a persone non autorizzate di visualizzare il vostro lavoro.

L'utilizzo di questi tipi fondamentali di password è obbligatorio. Imparatene l'utilizzo, e nel caso dobbiate comunicare, almeno temporaneamente, ai tecnici incaricati dell'assistenza, la vostra password registrate l'ora di comunicazione e di rinnovo della vostra password.

- **Attenzione alle stampe e ai fax di documenti riservati:** non lasciate accedere alle stampe o ai fax persone non autorizzate, se la stampante o il fax non si trovano sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Posizionate le stampanti e i fax in luoghi controllati e non accessibili al pubblico ed a visitatori. Distruggete personalmente le stampe quando non servono più. È opportuno l'utilizzo di una macchina distruggi documenti, indispensabile nel caso di documenti sensibili o giudiziari.

- **Non utilizzate le e-mail per dati riservati:** non inviate MAI dati sensibili o riservati via email come numeri di carta di credito, password, numeri di conti bancari.

- **Prestate attenzione all'utilizzo dei computer portatili:** i computer portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido e utilizzate una procedura di backup periodico. Se durante la giornata vi spostate molto dalla vostra postazione o addirittura la notte lasciate il vostro portatile in ufficio, riponetelo in armadi chiusi a chiave.
- **Non fatevi spiare quando state digitando la password:** anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete una buona capacità di digitazione.

- **Custodite la password in un luogo sicuro:** scrivete la vostra password, chiudetela in busta chiusa e consegnatela all'incaricato addetto alla sua custodia che provvederà a firmarla nei lembi di chiusura. Fate ben attenzione a non riscrivere la vostra password, l'unico affidabile dispositivo di registrazione è la vostra memoria.

- **Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità e delle loro autorizzazioni:** personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro computer.

- **Non utilizzate apparecchi non utilizzati:** l'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutti i dati dell'organizzazione. Per l'utilizzo consultatevi con il Responsabile del trattamento dati.

- **Non installate programmi non autorizzati:** solo i programmi acquistati dalla vostra organizzazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici consultatevi con il Responsabile del trattamento dati.

- **Adottate con cura le linee guida per la prevenzione di virus:** la prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di tutti i dati.

- **Controllate la politica locale relativa ai backup:** i vostri dati potrebbero essere gestiti su un server, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Chiedete al Responsabile del trattamento dati quali sono le operazioni di backup che dovete eseguire, con quali modalità e con quali tempi. Il Responsabile del trattamento curerà con estrema cura ed attenzione i backup periodici di tutti i dati.

- **Utilizzate gruppi di continuità:** verificare l'utilizzo di gruppi di continuità.

- **Segnalate le anomalie:** segnalate sempre, al più presto, al Responsabile del trattamento dati, qualsiasi tipo di anomalia si verifichi, sia nelle funzionalità del computer in cui operate, sia sulla rete di computer su cui operate, sia su qualsiasi altra applicazione che state utilizzando. Segnalare in tempo le anomalie e circostanziare gli eventi è fondamentale per prevenire problemi ben più consistenti.

Istruzione del Responsabile del Trattamento

Il Responsabile del trattamento è debitamente nominato dal Titolare del trattamento in osservanza alle disposizioni di cui all'art.28 del Reg. UE 2016/679.

Il Responsabile del trattamento dei dati personali deve scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio.

Principi generali da osservare

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale. Ai sensi dell'art.5 del Reg. UE 2016/679, che prescrive i "Principi applicabili al trattamento di dati personali" per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

I dati devono essere trattati:

- secondo il principio di **liceità**, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- secondo il principio di **trasparenza**, che consente all'interessato di venire a conoscenza delle metodologie e delle finalità di utilizzo dei propri dati;
- secondo il principio di **adeguatezza** il trattamento dei dati deve essere riferibile alla tipologia di incarico o mansione svolta;
- secondo il principio di **pertinenza**, ovvero, i dati devono essere trattati in relazione allo scopo 'cui sono destinati;
- secondo il principio della **limitatezza**, la raccolta dei dati non può eccedere ai dati strettamente necessari per la finalità perseguita.

I dati devono essere raccolti solo per **scopi**:

- **esatti**, cioè, precisi e rispondenti al vero e, se necessario, **aggiornati**;
- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli Atti amministrativi. Trascorso, detto periodo i dati vanno resi anonimi o cancellati e, la loro comunicazione, diffusione non è più consentita;
- **trattati** in modo tale che venga garantita un'adeguata sicurezza mediante misure tecniche ed organizzative adeguate;
- **determinati**, vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- **espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- **legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

In particolare, i dati idonei a rivelare lo **stato di salute** o la **vita sessuale** sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di **riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Ciascun addetto deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni di cui al Regolamento Europeo in materia di trattamento dei dati personali sono previste **sanzioni amministrative e pecuniarie** (art. 83). Per le altre sanzioni riferibili alle violazioni non soggette, amministrative e pecuniarie si rimanda alla legislazione nazionale.

In ogni caso, la **responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Mentre, in merito alla **responsabilità civile**, si fa rinvio all'art. 2050 del Codice Civile, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che per evitare ogni responsabilità, l'operatore è tenuto a fornire prava di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

Compiti particolari dell'addetto esterno
L'addetto esterno al trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare**:

- identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- definire, per ciascun trattamento di dati personali, **la durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita **l'informativa** ai soggetti interessati, ai sensi dell'artt.13 – 14 – 21del Regolamento;
- adempiere agli **obblighi di sicurezza**, quali attenersi alle disposizioni di cui agli artt. 25 e 32 del Regolamento, cioè adottare le misure di sicurezza idonee per adottare tutte le **preventive misure di Sicurezza** ritenute **idonee** al fine di ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- **comunicare** tempestivamente al Titolare del trattamento casi di **accesso non autorizzato** ai dati o di trattamento non consentito o non conforme alle finalità perseguite;
- far osservare gli adempimenti previsti in caso di **nuovi trattamenti e cancellazione** di trattamenti;
- segnalare al Titolare del trattamento l'eventuale **cessazione di trattamento**.

In merito agli addetti, l'addetto esterno deve:

- individuare, tra i propri collaboratori, designandoli per iscritto, addetti al trattamento fornendo loro le **istruzioni** a cui devono attenersi per svolgere le operazioni di trattamento;
- **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli addetti del trattamento, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza da parte degli addetti, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli addetti, avendo cura di adottare preventivamente le misure organizzative idonee e impartite

le necessarie istruzioni ai fini di riscontro di eventuali richieste di esecuzione dei diritti di cui all'art. 5, agli artt. 12 e ss. Fino al 22 e all'art. 34;

- evadere le eventuali richieste di **accesso**, rettifica, integrazione, cancellazione, blocco dei dati da parte dell'interessato che eserciti i propri diritti ai sensi degli artt. di cui sopra;

- collaborare con il Titolare del trattamento all'adempimento degli obblighi previsti dal Regolamento e segnalare eventuali problemi applicativi.

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 si trasmette un virus:
- attraverso programmi provenienti da fonti non ufficiali;
- attraverso le macro di alcuni programmi;
- attraverso le e-mail ricevute;
- attraverso il download da Internet.

Come NON si trasmette un virus:
- attraverso file di dati non in grado di contenere macro (file di testo, pdf, jpeg, etc.);
- attraverso e-mail non contenenti allegati.

Quando il rischiò da virus si fa serio:
- quando si installano programmi;
- quando si copiano dati, dai dischi;
- quando si scaricano dati o programmi da internet.

Quali effetti ha un virus?
- Effetti sonori e messaggi sconosciuti appaiono sul video;
- Nel menù appaiono funzioni extra finora non disponibili;
- Lo spazio sul disco si riduce inspiegabilmente;
- Le funzionalità dei computer rallentano repentinamente.

Come prevenire i Virus

- **Usate 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 utilizzare programmi non autorizzati dal Responsabile del trattamento dei dati.
- **Assicuratevi di non far partire accidentalmente il vostro computer da Cd o DVD:** infatti se la fonte fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.
- **Assicuratevi che il vostro software antivirus sia aggiornato:** la tempestività nell'azione di bonifica è essenziale per limitare danni che un virus può causare; inoltre è vitale che il programma antivirus sia aggiornato periodicamente (non oltre una settimana).
- **Assicuratevi che sul vostro computer sia attivato il Firewall:** verificate dalle preferenze del vostro computer o chiedete al Responsabile del trattamento dati, che sul vostro computer sia attivato il Firewall e solo i privilegi di rete minimi necessari alle vostre esigenze di accesso ai dati, oltretutto se sul vostro computer non vi collegate ad Internet o non inviate fax staccate il cavo telefonico per evitare possibili accessi
- **Non diffondete messaggi di provenienza dubbia:** se ricevete messaggi che avvisano di un nuovo virus pericolosissimo e che fanno riferimento ad una notizia proveniente dalla "Microsoft", ignoratelo, le email di questo tipo sono dette con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala")

- **Non partecipate a "catene di S. Antonio" e simili:** analogamente, tutti i messaggi che vi invitano a "diffondete 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, per ciò utilizzare indebitamente le risorse informatiche.
- **Non aprite allegati alle e-mail inviate da sconosciuti:** non aprite allegati alle e-mail con file di tipo Excel, Zip, Word contenente macro e qualsiasi altro formato a voi sconosciuto se non siete certissimi della provenienza. Potete aprire solamente allegati di tipo pdf, jpg e file di testo che non contengono macro.

Scelta delle Password

Il più semplice metodo per l'accesso illecito ad 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 non protetto da password "poco sicura". La scelta di password "sicure" è quindi, parte essenziale della sicurezza informatica

Cosa NON fare

- **NON dite a nessuno la vostra password.** Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
- **NON scrivete la password da nessuna parte** che possa essere letta facilmente, soprattutto vicino al computer.
- **NON scegliete password che si possano trovare su un dizionario.** Su alcuni sistemi è possibile provare tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- **NON crediate che usare parole straniere renderà più difficile il lavorò di scoperta**, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- **NON usate il Vostro nome utente.** È la password più semplice da indovinare.
- **NON usate password che possono in qualche modo essere legate a Voi** come, ad esempio, il Vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di, telefono, ecc.

Cosa fare

- Cambiare la password a intervalli regolari. La normativa sulla privacy prevede che se sono trattati dati sensibili o giudiziari la password deve essere cambiata ogni tre mesi altrimenti ogni sei mesi. La password deve essere lunga almeno otto caratteri, meglio se con un misto di lettere, numeri e segni di interruzione.
- Utilizzate password distinte per l'accesso a vari sistemi.
- Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe.