Dr.ssa *Alessandra Piccolo*
Data Protection Officer - ASP Messina
dpo@asp.messina.it

Fondamenti della protezione dei dati: buone prassi e piccole regole nell'utilizzo degli strumenti

Premessa

Questo documento ha lo scopo di ricordare come dei piccoli accorgimenti possano essere fondamentali nel rispetto della gestione dei dati e della sicurezza delle informazioni. All'inizio possono apparire inutili o cose risapute ma purtroppo, nella quotidianità lavorativa hanno un peso sia dal punto di vista delle buone prassi, sia da quello della responsabilità che la loro inosservanza può determinare.

Buone Prassi

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 anche vero che pone, se non altro, un primo ostacolo. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, **chiudere a chiave il vostro ufficio quando non è presidiato scoraggia sicuramente intrusioni indesiderate.**

I documenti contenenti dati personali e particolari, come adesso sono chiamati dal GDPR 2016/679, **vanno riposti negli appositi archivi**, non è conveniente lasciare, al termine delle operazioni affidate, le pratiche sulla scrivania o in luoghi diversi da quelli deputati ad accoglierli. **Non possono accedere** alla **fotocopiatrice**, alla **stampante,** al **fax**, persone non autorizzate ed è fondamentale ritirare i documenti elaborati da questi strumenti. Lasciarli incustoditi significa diventare responsabili della loro perdita, sottrazione e divulgazione.

Non si possono consegnare copie fotostatiche o di altra natura, a persone non autorizzate dal Titolare/Responsabile del trattamento.

Quando si devono **portare documenti da un ufficio** all'altro è importante che non siano visibili dati personali e che vengano utilizzate tutte le precauzioni del caso: carpette anonime, faldoni impersonali ecc…

Il periodico **smaltimento di materiale cartaceo** contenente dati personali deve essere effettuato con alcune cautele. Occorre evitare che le informazioni personali possano essere utilizzate da persone non legittimate. A tal fine occorre aver cura che: le eventuali copie di documenti, di scritti, di appunti, di tabulati di prova, etc., non più utilizzati vengano eliminati con l'apposita **macchina distruggi documenti o in mancanza ridotti in "coriandoli";** i documenti così distrutti devono essere inseriti in contenitori chiusi (buste, scatoloni, etc.) senza specifiche indicazioni del contenuto; i contenitori dovranno essere ritirati dal personale autorizzato.

Dr.ssa *Alessandra Piccolo*
Data Protection Officer - ASP Messina
dpo@asp.messina.it

Uso corretto dell'hardware

Proprietà del computer e dei dati nello stesso contenuti. Tutti i computer, incluso altro hardware, nonché i dati e il software nello stesso contenuti (di seguito chiamato "PC"), sono di proprietà dell'ASP Messina e sono forniti allo scopo di svolgere le mansioni affidate.

Ogni informazione contenuta o memorizzata in qualsiasi PC cui si abbia accesso, di diversa natura e correlati all'attività dell'ASP, non possono essere riprodotte o divulgate senza apposite autorizzazioni.

Utilizzo di software. Non si può usare, installare o copiare nel PC affidato dall'ASP alcun software che non sia stato fornito dall'Ente stesso o il cui uso non sia stato da questa autorizzato.

Sicurezza del PC. E' necessario impegnarsi a fare tutto il possibile per evitare l'accesso al PC a terzi non autorizzati e a mantenere la natura riservata delle Informazioni confidenziali.

La digitazione della password deve avvenire in modo discreto, anche se i programmi non ripetono in chiaro la password sullo schermo, questa potrebbe essere letta guardando i tasti che state digitando, anche se avete buone capacità di dattiloscrittura.

Non scrivete la password da nessuna parte, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria o un supporto al quale è difficile accedere. Non effettuate, sotto Windows, la memorizzazione automatica delle password ma digitatele ogni volta che vi vengono richieste.

Utilizzate un salvaschermo che possa attivarsi dopo pochi minuti di inattività.

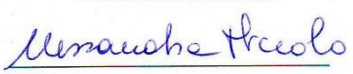
Il Personale esterno può avere bisogno di **installare nuovo hardware/software nel vostro computer**, **è necessario assicurarsi dell'identità della persona** e delle autorizzazioni ad operare sul vostro PC.

Molti programmi applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, è buona prassi prendere l'abitudine di salvare direttamente i documenti in fase di elaborazione in modo da gestire personalmente i dati e non fare esclusivo affidamento sul sistema.

Per i dispositivi elettronici (cd-rom, pen drive ecc…) si applicano gli stessi criteri dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli. Non possono essere utilizzate pen drive per il trasferimento di dati particolari/sensibili a meno che non siano protette con sistemi di crittografia.

Messina, 07/06/2018

Dr.ssa Alessandra Piccolo



(D.P.O. ASP Messina)