MANSIONARIO COMPORTAMENTALE
a tutela e protezione dei dati personali

Il trattamento dei dati personali, e a maggior ragione quelli sensibili e giudiziari, deve essere ricondotto a:

1) **riservatezza** (garanzia che il dato sia trattato solo da colui che ne è autorizzato),
2) **integrità** (garanzia che il dato sia quello che è stato trattato originariamente),
3) **disponibilità** (garanzia che il dato sia sempre reso disponibile all'utilizzatore concretamente autorizzato).

In quest'ottica si inserisce il concetto di **sicurezza dei dati**, specificando che con il termine "sicurezza" s'intende l'insieme di misure, di carattere **organizzativo e tecnologico**, adeguate ad assicurare a ciascun utente autorizzato esclusivamente i servizi previsti per l'utente stesso, nei tempi e nelle modalità stabilite.

Secondo la nota definizione ISO, la sicurezza è "**l'insieme delle misure atte a garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite**" e dunque l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco, così riducendo il rischio.

Il **titolare dei dati** e/o il **responsabile del trattamento dei dati**, in funzione di quanto appena detto, ha l'obbligo di effettuare un'attenta analisi dei rischi, valutando opportunamente tutte le minacce e le relative vulnerabilità che possono concretizzarsi in uno o più "attacchi" ai dati. A valle di questa analisi è onere individuare le opportune contromisure per contrastare/minimizzare gli attacchi, in modo da ridurre il rischio, ricordando che in caso di controllo da parte del Garante occorrerà dimostrare la propria perfetta buona fede.

Per prevenire gli attacchi è necessario che gli **incaricati del trattamento dei dati** utilizzino idonee misure di sicurezza, per evitare che estranei, appropriandosi di informazioni, possano esporre, a sanzioni civili e penali, loro stessi nonché lo stesso titolare dei dati.

Si ricorda, infatti, che l'attività di trattamento dei dati personali è qualificata dalla Magistratura ordinaria di merito come attività pericolosa, disciplinata dal Codice Civile, ed in caso di richiesta di risarcimento del danno da parte del soggetto che si ritiene leso dalle modalità del trattamento dei propri dati, è il titolare del trattamento tenuto a fornire la prova di avere adottato le misure idonee ad evitare il danno.

Per ridurre il rischio occorre adottare le seguenti misure di sicurezza:

- utilizzare una **password di accesso** sul proprio PC, di **otto caratteri alfanumerici**, evitando di assemblare in essa elementi della propria vita privata e/o comunque a essa riconducibile;
- cambiare la password **ogni tre mesi**, trattando dati sensibili e/o giudiziari (altrimenti, per i dati personali, ogni sei mesi);
- **attivare una password di screen saver**, quando il proprio PC già in uso durante la sessione di lavoro non è presidiato, ricordando che l'avviamento della stessa è *sub judice* ad un lasso di tempo di attivazione che non tutela l'incaricato del trattamento; si consiglia, pertanto, alla bisogna, di attivarla manualmente, premendo contemporaneamente i tasti Windows + L (Figura 1);


Figura 1

- evitare di comunicare a chicchessia la propria password; la propria password dev'essere trascritta su di un foglio e dev'essere consegnata, in **busta chiusa** (sigillata e controfirmata sui lembi di chiusura), al **custode delle Password**;
- il custode delle Password dovrà annotare su un **registro delle Password** le date in cui le stesse sono state cambiate al fine di darne evidenza oggettiva in caso di controlli da parte del Garante;

- prima e dopo il trattamento, evitare di lasciare **informazioni cartacee incustodite** sulla propria scrivania e custodirle in armadi e/o cassettiere muniti di serratura;
- accertarsi che gli armadi/cassettiere muniti di serratura, siano rigorosamente sempre chiusi a chiave prima, durante e dopo l'operazione di trattamento;
- ricordare che il dato elettronico e il dato cartaceo sono sempre sostanzialmente equiparati e, pertanto, qualsiasi dato stampato ed incustodito equivale ad un accesso al proprio PC, anche se spento;
- proteggere i dati (elettronici e cartacei) **chiudendo a chiave la propria stanza**;
- ricordare che le stanze di lavoro, spesso, vengono pulite da personale esterno all'azienda e, soprattutto, non in presenza degli incaricati del trattamento dei dati;
- utilizzare sempre un criterio di cifratura, quale per esempio la separazione del dato personale da qualsiasi fattore che violi la dignità dell'individuo, adottando, per esempio, le iniziali del nome/cognome se associato a componenti che contrastino l'art. 11 del D. Lgs. 196/03 e s.m.i., in riferimento a qualsiasi interessato del trattamento;
- consegnare referti, cartelle cliniche, ecc. solo all'interessato o a persona espressamente o preventivamente delegata;
- provvedere ad aggiornare o far aggiornare, almeno settimanalmente se non quotidianamente, l'antivirus, il firewall, l'antispamming, ecc. (l'attività, nell'ASP di Catanzaro, è garantita dal livello centrale);
- evitare di installare software, anche free, se non espressamente autorizzato dall'Amministratore di rete;
- è vietato avvalersi di amici e/o esperti di informatica, esterni alla propria struttura, facendoli intervenire sul proprio PC, per qualsivoglia motivo;
- avvalersi di personale, individuato dal Titolare dei dati, per la manutenzione del proprio PC, provvedendo a farlo manutentare in loco e in presenza dell'interessato al trattamento o di personale opportunamente delegato;
- evitare, ove possibile, di trasferire dati personali all'esterno del perimetro di sicurezza, dove esiste una protezione (organizzativa, fisica e logica) del proprio ambito lavorativo;
- ricordare che i supporti removibili (HD esterni, chiavi USB, CD-ROM, ecc.) non sono sufficientemente protetti e, pertanto, vanno custoditi diligentemente e se non più utilizzati devono essere distrutti;
- effettuare almeno settimanalmente il salvataggio di quei dati che risiedono sul proprio PC e non sono salvati sui Server, provvedendo ad una conservazione sicura dei supporti che li contengono ed in posti diversi da dove è ubicato ogni singolo PC.

Catanzaro, 15 maggio 2019

Il Responsabile della Protezione dei Dati
Dr Piercarlo Rizzi