P 3888
DEL 10 MAG 2018

COMUNE DI MARANO PRINCIPATO

(Provincia di Cosenza)

ALL. A

Ai Sigg. Responsabili dei Settori
Ai Sigg.ri Dipendenti Comunali
con postazioni informatiche
SEDE

OGGETTO: D. Lgs. 196/2003 e ss.mm. Regolamento UE Privacy 679/2016 –Direttive per la custodia dei dati.

Il Codice Privacy distingue tra trattamenti effettuati con:

- strumenti **elettronici**, termine nel quale la lettera b) del comma 3 dell'articolo 4 fa rientrare gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- strumenti **diversi da quelli elettronici**: faldoni nei quali sono racchiuse pratiche, schedari nonché simili, e tuttora assai diffusi nonostante si sia in piena rivoluzione virtuale, mezzi tradizionali di annotazione, conservazione e consultazione di informazioni e dati.

Le misure minime di sicurezza per i trattamenti effettuati con strumenti elettronici sono prescritte dall'articolo 34 del codice privacy. In tale categoria rientrano gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Il Codice intende per:

- "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica. Alcuni esempi di credenziale sono l'impronta digitale, la forma della mano, l'iride, la retina, la voce (caratteristiche **biometriche**), certificati digitali memorizzati su smart card, un codice identificativo (*username*) associato ad una *password.*
- "**profilo di autorizzazione**", l'insieme delle informazioni associate ad una persona, che consente di individuare a quali dati e a quali trattamenti la stessa può accedere.

E' bene precisare la differenza tra **autenticazione** ed **autorizzazione**: il sistema di autenticazione, si accerta dell'identità dell'utente, al fine di consentire o meno l'acceso al computer; con il sistema di autorizzazione si stabilisce a quali dati del computer l'incaricato può accedere, dopo che è entrato, e quali azioni (trattamenti) può compiere.

Autenticazione, codici identificativi e password

Visto che sistemi di autenticazione basati sulla coppia username+password, risultano fra i più rapidi ed economici da approntare, è utile approfondire l'argomento.
Il **codice per l'identificazione dell'incaricato** è il nome grazie al quale l'utente viene riconosciuto dal sistema; deve essere unico per ogni incaricato, non può essere assegnato a differenti incaricati anche in tempi diversi e, eventualmente, deve essere disattivato se non usato per più di sei mesi o se l'incaricato perde tale qualifica.
La **Parola chiave** è la tipica password. Si tratta di una parola segreta conosciuta solo dall'incaricato che permette di verificare che l'utente che chiede di accedere al sistema sia proprio la persona associata al codice identificativo di cui sopra. Gli incaricati devono conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione.
La parola chiave dovrà:

- essere costituita da almeno otto caratteri o comunque dal numero di caratteri consentiti dal sistema se inferiore a otto, e non deve contenere riferimenti direttamente riconducibili all'incaricato: non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici. E' buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica.
- essere modificata al primo utilizzo, non appena comunicata per la prima volta da chi amministra il sistema e, successivamente, ogni sei mesi nel caso di dati personali, mentre nel caso di dati sensibili o giudiziari la modifica dovrà intercorrere ogni novanta giorni. Nessun altro, neppure il titolare del trattamento, può accedere allo strumento elettronico, utilizzando la credenziale di autenticazione dell'incaricato. Eccezione a tale regola si ha solo se verificano congiuntamente le seguenti condizioni:

Prolungata assenza o impedimento dell'incaricato.

Considerato che occorre comunque garantire l'operatività e la sicurezza del sistema, il titolare deve prendere le opportune misure, per essere in grado di accedere ai dati ed agli strumenti, al verificarsi delle condizioni sopra esposte. A tale fine, agli incaricati devono essere fornite istruzioni scritte, affinché:

- predispongano 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 e, possibilmente, sigillata);
- consegnino tale copia ad un soggetto, che sia stato previamente incaricato della sua custodia (l'incaricato per la custodia delle parole chiave). Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere, all'incaricato per la custodia, la busta che la contiene. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Inoltre, è importante che gli operatori siano edotti circa i rischi derivanti da:

- memorizzazione di credenziali per l'accesso a siti internet sfruttando l'apposito meccanismo offerto dai sistemi operativi Windows. Chiunque abbia accesso alla postazione di lavoro può recuperare dette credenziali con estrema facilità;
- utilizzazione delle stesse credenziali per l'autenticazione su sistemi differenti;
- principali tecniche di "spoofing" (furto di credenziali realizzato mediante e-mail e siti fraudolenti);

- installazione di software senza l'autorizzazione dell'amministratore di sistema. Oltre alle problematiche legate a virus ed affini, va evidenziata la perdita di sicurezza derivante dall'installazione di programmi per la condivisione di file o la tele-assistenza.

Altre disposizioni

Lo strumento elettronico non dovrà essere lasciato incustodito e accessibile durante una sessione di trattamento qualora l'incaricato debba assentarsi dalla propria postazione per un periodo più o meno prolungato. Il "trattamento" non consiste infatti solo nella modifica o copia del dato: anche la semplice presa visione può essere considerata, a tutti gli effetti, trattamento. Da tale prescrizione non consegue l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare. Si devono però mettere 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;
- **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. Altra soluzione potrebbe essere l'utilizzo di uno screensaver con password.

Il disciplinare prevede l'obbligo di proteggere i dati personali contro il rischio di intrusione e dall'azione di programmi che possono portare al danneggiamento di un sistema informatico, dei dati o dei programmi in esso contenuti. Per ovviare al pericolo di intrusione informatica e cioè di tentavi dall'esterno di accesso non autorizzato al nostro sistema informatico ci si può affidare ai **firewall**. I firewall sono dei sistemi di tipo hardware o software. Il loro lavoro in sostanza lo si può paragonare ad un guardiano che vigila la porta che utilizziamo per "uscire" dal nostro sistema informatico per accedere ad altri (ad esempio ogni qualvolta navighiamo in internet), impedendo che "qualcuno" non autorizzato possa entrare di soppiatto.

Per quanto riguarda il pericolo di danneggiamento di un sistema informatico è chiaro che si sta facendo riferimento all'azione dei virus informatici. La norma impone di difendersi impiegando uno dei vari software antivirus in commercio alla cadenza "almeno semestrale". Comunque gli antivirus di ultima generazione utilizzano un sistema di aggiornamento automatico che consente di essere tempestivamente protetti appena un nuovo virus viene messo in circolazione.

Importante è procedere all'aggiornamento dei "programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti", che dovrà essere effettuato annualmente o, nel caso si trattino dati sensibili o giudiziari, semestralmente. I nuovi sistemi operativi hanno incorporato una funzione automatica che avvisa quando la casa madre ha rilasciato una nuova "patch" sollecitando l'utente alla sua installazione in modo da procedere all'aggiornamento.

Adozione tecniche di cifratura o di codici identificativi

Quando si trattano dati sensibili idonei a rivelare lo stato di salute o la vita sessuale, si impone l'adozione di tecniche di cifratura o l'utilizzo di codici identificavi allo scopo di rendere i dati difficilmente interpretabili.

Backup

Per quanto riguarda "il salvataggio dei dati" con una cadenza almeno settimanale, il recupero dei dati al verificarsi di eventi atti a distruggerli deve essere sempre previsto per far si' che, in caso di problemi, non venga meno uno degli obiettivi principali della sicurezza nel trattamento dei dati (la disponibilità dei dati stessi).

Ai supporti rimovibili (es: pen-drive, cdrom,) contenenti dati sensibili o giudiziari è richiesta una particolare attenzione. Questi devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati e trattamenti non consentiti: ad esempio, essi vengono conservati in cassetti chiusi a

chiave e successivamente, quando è cessato lo scopo per cui sono stati memorizzati, i dati dovranno essere cancellati. I cdrom non riscrivibili dovranno essere distrutti. Si consiglia di seguire le prescrizioni in commento anche per i supporti contenenti solo dati comuni.
Per quanto riguarda il backup di dati sensibili e giudiziari, l'organizzazione deve essere in grado di provvedere in ogni caso al ripristino dei dati entro sette giorni. I soggetti esterni che, professionalmente, assistono il titolare nella predisposizione ed installazione delle misure minime di sicurezza, devono rilasciare un certificato di conformità, nel quale devono descrivere quale sia stato l'intervento effettuato. La disposizione è atta a garantire la serietà degli interventi, rispetto a quanto richiesto dal disciplinare tecnico.
E' opportuno, pertanto, effettuare backup differenziali o incrementali infrasettimanali ed un backup completo settimanale.

Interventi formativi

Gli **interventi formativi degli incaricati del trattamento** devono essere programmati in modo tale che essi abbiano luogo almeno al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti rispetto al trattamento di dati personali.

Gli interventi formativi, che possono avvenire all'interno e/o presso soggetti esterni specializzati, devono essere finalizzati a rendere gli incaricati edotti dei seguenti aspetti:

- ✓ 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.

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
19. Il Comune di Marano Principato ha realizzato il sito web comunale al fine di consentire al cittadino, attraverso una grafica semplice e chiara, una migliore consultazione e navigazione e quindi un più facile accesso ai servizi comunali.
    Ai sensi e per gli effetti della L. 134/2012, della L. 190/2012 la Pubblica Amministrazione ha l'obbligo di pubblicare on-line, in apposita Sezione del Sito Web comunale, tutti gli atti amministrativi, documenti, informazioni, ecc..., per consentire la più ampia e facile accessibilità a chiunque. Gli atti contenenti informazioni sensibili devono essere "depurati" dalle indicazioni soggette a particolare tutela per la privacy, garantendo all'uopo misure di anonimizzazioni (es. stralciare il Codice IBAN del fruitore, il codice fiscale, le iniziali del nome e del cognome, ecc...).
    La pubblicazione dei dati sul sito deve essere effettuata nel rispetto della normativa in materia di "protezione dei dati personali" garantendo che i dati pubblicati e i modi di pubblicazione siano pertinenti e non eccedenti rispetto alle finalità indicate nella legge. Si provvederà, pertanto, ad archiviare i dati non più aggiornati e, relativamente ai dati sensibili, verranno utilizzate modalità che ne tutelino l'anonimato fermo restando il divieto di pubblicare i dati idonei a rivelare lo stato di salute dei singoli interessati.
    La rete internet ed intranet non devono essere utilizzati per scopi incompatibili con l'attività istituzionale del Comune.
    E' vietata la diffusione di dati non pertinenti rispetto alle finalità non perseguite.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

19. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
20. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
21. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
22. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
23. Il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati deve avvenire con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.

Misure di tutela e garanzia

24. Il titolare che adotta misure minime di sicurezza, avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione, riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
25. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

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

26. Agli incaricati 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 incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
27. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati 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.
28. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Le norme in materia di protezione dei dati personali distingue due distinti obblighi:

a) **L'obbligo più generale di ridurre al minimo determinati rischi:**
   occorre custodire e controllare i dati personali oggetto di trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dai casi consentiti o altrimenti trattati in modo illecito. Oltre alle cosiddette "misure minime" di sicurezza sussiste l'obbligo di adottare ogni altra misura di sicurezza idonea a fronteggiare le predette evenienze anche in base alle conoscenze acquisite in base al progresso tecnologico, alla natura dei dati e alle caratteristiche del trattamento, di cui si devono valutare comunque i rischi.
   L'inosservanza di questo obbligo rende il trattamento illecito.
b) **Nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "misure minime".**
   Occorre assicurare comunque un livello minimo di protezione dei dati personali.

Il Sindaco
Dott. Luigi Pulice