

Allegato 6

PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

Documento Programmatico sulla sicurezza ai sensi del decreto legislativo 196/2003 e successive modifiche.

Finalità del documento :

Delineare il quadro delle misure di sicurezza organizzative fisiche e logiche da adottare al fine del trattamento dati personali effettuato dal Comune di Montecrestese

Si definiscono le seguenti figure:

Titolare del trattamento : Sig.ra Perego Margherita: responsabile segreteria

Responsabile del trattamento: Sig.ra Migliarini Daniela ruolo: responsabile del procedimento

Responsabile esterno: Sig. Riva Davide, titolare della ditta Cobaltool che effettua il Backup giornaliero.

Conformemente a quanto prescrive il punto 19. del Disciplinare tecnico, allegato sub b) al Decreto Legislativo 196/2003 e nel rispetto dello schema di compilazione suggerito dal Garante, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
 - * la individuazione dei tipi di dati personali trattati
 - * la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
 - * l'elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti
 - * Le indicazioni di massima del tipo di dati trattabili
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati (punto 19.2 del disciplinare)
3. l'analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare)
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati (punto 19.4 del disciplinare)
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento (punto 19.3 del disciplinare)
6. la previsione di interventi formativi degli incaricati del trattamento (punto 19.6 del disciplinare)
7. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno (punto 19.7 del disciplinare)
8. le procedure da seguire per il controllo sullo stato della sicurezza
9. dichiarazioni d'impegno e firma.

Indicazioni generali ai dipendenti e agli incaricati del trattamento interni ed esterni:

- i dati sensibili sono : i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. I provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del Dpr 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- I dati personali oggetto di trattamento devono essere:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- c) esatti e, se necessario, aggiornati;
- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

Analisi dei rischi

- I rischi potenzialmente più probabili di sottrazione di dati privati da noi posseduti sono :
- Prelievo non autorizzato via Internet
- Prelievo non autorizzato da parte dei dipendenti o delle della ditta esterna incaricata della manutenzione
- Sottrazione supporti di backup
- Sottrazione di personal computer
- L'attività di monitoraggio dei rischi è a cura del Sig.. Riva Davide.
-
- Punti di accesso e stazioni base
- Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
- Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing).
- Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

Procedure di sicurezza interne adottate :

- Aggiornamento annuale dei programmi antivirus
- Protezione dell'accesso internato con firewall hardware e software
- Tutti i computer sono protetti da Antivirus e/o firewall
- Aggiornamento come minimo settimanale delle definizioni dei programmi antivirus e di protezione , aggiornamento di tutte le patch di sicurezza Microsoft.
- Protezione tramite password strettamente personale dell'accesso ai sistemi contenenti dati protetti da privacy sostituita ogni 90 giorni.
- Protezione tramite firewall dell'accesso alla rete internet
- Salvataggi giornaliero di tutti i dati protetti da privacy su hard disk in raid con accesso autorizzato al solo Sig. Riva Davide.
- Tutti i salvataggi sono criptati da password al fine di minimizzare i rischi in caso di furto o smarrimento.
- Il salvataggi dovranno essere in duplice copia. Almeno trimestralmente un salvataggio globale sarà trasferito su hard disk esterno e depositato in cassaforte.

ASPETTI DI SICUREZZA INFORMATICA

PER LA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

FORMAZIONE DEI DOCUMENTI

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno degli Uffici.

I documenti sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

Si adottano preferibilmente i formati PDF, XML e TIFF. I documenti informatici prodotti dall'A00 con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno dell'UP, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 (Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.).

I documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione.

GESTIONE DEI DOCUMENTI

Il sistema di protocollo informatico assicura:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di protocollo informatico consente:

- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PdP - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie

legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (firewall);
- dalle registrazioni del PdP.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RGD e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno degli UU o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Lo scambio per via telematica di messaggi protocollati tra UU di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

Scambio dei documenti all'esterno dell'amministrazione (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.

Ogni messaggio protocollato deve riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. Tali informazioni sono incluse nella segnatura informatica di ciascun messaggio protocollato e sono codificate in formato XML.

Con provvedimento dell'Agenzia per l'Italia Digitale, vengono indicati le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai messaggi protocollati.

Scambio dei documenti all'interno dell'amministrazione

Gli Uffici dell'amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l' "impiego della posta elettronica nelle pubbliche amministrazioni".

ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Il PdP adottato dall'amministrazione:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Accesso al registro di protocollo per utenti interni all'amministrazione

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

Un utente può avere la visibilità completa sul registro di protocollo solo a seguito di abilitazione.

Il personale dell'ufficio protocollo generale e dell'ufficio sistemi informatici sono abilitati alla visualizzazione completa sul registro protocollo.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. Nel caso in cui sia effettuata la registrazione di un documento riservato, la visibilità completa sul documento stesso è possibile solo alla persona destinataria del documento.

Di norma tutti gli utenti che devono protocollare sono abilitati alla consultazione, inserimento e modifica, ma è possibile abilitare un utente anche alla sola consultazione.

Solo il personale dell'ufficio Sistemi Informatici è invece abilitato all'annullamento.

CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Per la conservazione dei documenti informatici si applicano le regole di cui al decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.).

Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta all'interno della struttura organizzativa del soggetto produttore dei documenti o affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

L'amministrazione ha optato per la seconda soluzione ed ha richiesto ed ottenuto, da parte della Soprintendenza Archivistica territorialmente competente, il nulla-osta preventivo alla sottoscrizione di un Accordo di collaborazione con il Servizio Polo Archivistico Regionale dell'Emilia-Romagna ai fini della conservazione dei documenti informatici su piattaforma digitale.

Per le modalità operative di trasmissione del contenuto del pacchetto di versamento al sistema di conservazione si rimanda al manuale di conservazione.

Il manuale di conservazione inoltre illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.