

Comune di Campanium
Provincia di Napoli

Documento Programmatico sulla Sicurezza

Anno 2005

Capitolo I
Elenco dei trattamenti dei dati personali
Distribuzione dei compiti e delle responsabilità
(ex Dlg.196 30 giugno 2003 - All.B - regole 19.1 – 19.2)

Paragrafo 1 - Archivi dei Dati Personali trattati nel Comune di Campanium

Il Comune di Campanium è organizzato per macro aree di competenza, ciascuna delle quali opera nell'ambito di procedure operative istituzionalizzate e dispone di propri archivi di dati. Esse sono qui di seguito elencate:

Segreteria Affari Generali e Servizi Demografici

Dirigente Responsabile: Dott. Vincenzo Casale, Vice Segretario Comunale

Scuola e Servizi Sociali

Dirigente Responsabile: Dott. Mario Rossi, Segretario Generale

Finanze Tributi e Patrimonio

Dirigente Responsabile: Dott. Aldo Bianchi

Polizia Municipale, Servizi di Nettezza Urbana

Dirigente Responsabile: dott. Gaspare Spini

Ufficio Tecnico

Dirigente Responsabile: Ing. Giulio Torre

A seguito vengono elencate in apposite tabelle (All.) gli archivi dei dati di competenza e responsabilità di ciascuna area.

Paragrafo 2 – Descrizione del Sistema Informativo Comunale

Ai fini della valutazione della sicurezza dei dati trattati e custoditi nel Comune di Campanium, nel presente paragrafo vengono descritte l'architettura e la struttura funzionale del Sistema informativo Comunale.

Il Sistema Informativo del Comune di Campanium è costituito:

da un Sistema Informatico, ovvero dai computer e dalle reti fisiche di collegamento (hardware);

da Sistemi Operativi di Base, che hanno il compito di assicurare le funzioni fondamentali di affidabilità degli archivi elettronici, l'interconnessione e lo scambio delle informazioni, l'efficienza e la versatilità generale del sistema (software di base);

dal Sistema delle procedure applicative, che assicurano funzioni di impiego aderenti alle esigenze organizzative e operative del Comune (software applicativo).

Il Sistema Informativo Comunale, ovvero il complesso delle funzioni e delle procedure, dei metodi e delle strategie di gestione, di manutenzione

e di impiego delle risorse hardware e software in sintesi richiamate nelle righe precedenti, è sotto la responsabilità del Dirigente Dott. Vincenzo Castaldo;

Il responsabile operativo del Centro Elaborazione Dati è il sig. Nicola De Laurentiis.

Il Sistema Informatico del Comune di Campanium è articolato in circa 120 Posti di Lavoro, ciascuno corredato di Personal Computer, collegati in un sistema di reti locali interconnesse del tipo RJ45, secondo il protocollo di trasmissione dati TCP/IP. La rete locale nel suo complesso fa capo ad un Server Web, o di rete, su cui sono gestite le connessioni con l'esterno (Internet), e ad un Server applicativo, che custodisce gli archivi, che gestisce la struttura delle password di accesso, e che ospita le procedure di salvataggio dati.

Allo stato attuale i posti di lavoro del comune di Campanium sono equipaggiati con PC di molte e differenti generazioni tecnologiche, e pertanto i Sistemi Operativi su di essi installati sono sia prodotti software di più recente generazione, quali:

Microsoft Windows 2000[®] Professional

Microsoft Windows XP[®] Professional

sia Sistemi Operativi di rilascio precedente, quali:

Microsoft Windows '98

Microsoft Windows '95

Microsoft Windows ME

Poiché in questi ultimi casi le tecniche di registrazione e classificazione dei dati sui supporti magnetici non consentono una adeguata protezione agli accessi in relazione alla necessità di autenticazione degli utenti¹, il Comune di Campanium, prendendo atto della presente situazione, si impegna a disporre – nei limiti consentiti dalle disponibilità di bilancio – i piani di sviluppo e gli interventi tecnici e finanziari finalizzati alla riconversione tecnologica resa necessaria dalle disposizioni della Legge.

Il Sistema Applicativo installato sulla rete Comunale è costituito da una suite ERP (Enterprise Resource Planning) per Enti Pubblici – il cui nome è DELISA - fornita dalla Società Info Servizi, che ne ha curato altresì la personalizzazione, la configurazione e l'installazione sui PC della rete. La Info Servizi ha fornito inoltre corsi introduttivi di addestramento alle procedure.

Ai fini della Sicurezza e della Protezione dei Dati – con particolare riferimento alla protezione dei Dati Personali e Sensibili contenuti sulla rete, il Sistema Informativo dispone delle potenzialità a seguito elencate:

un dispositivo Firewall, installato presso il Server Web di collegamento con l'esterno, a monte della rete, che – adeguatamente configurato – ha il compito di sbarrare l'accesso a programmi, messaggi e posta indesiderata, che possono introdursi dall'esterno per danneggiare o carpire le informazioni comunali;

una configurazione dei server di gestione degli archivi che contiene procedure di attivazione automatica e periodica di salvataggio (backup) dei dati;

una configurazione delle condivisioni degli archivi strutturata in modo che da ciascun posto di lavoro si possano attingere dati e informazioni soltanto se congruenti e funzionalmente connesse alle funzioni svolte;

¹ vedi Articolo 34 del Dlg.196/2003: misure minime di sicurezza

un sistema di autenticazioni personali² (password) che identificano funzionalmente oltre che personalmente l'utente che accede alla rete, cosicchè egli possa da qualsiasi punto di accesso essere identificato e autorizzato ad accedere unicamente agli archivi e alle procedure previste dalla propria specifica autenticazione;

un sistema di programmi di protezione Antivirus installato su tutti i PC della rete e regolarmente aggiornati;

un Portale comunale, dotato di link verso i corrispondenti istituzionali di più comune e rilevante collegamento (prefettura, regione, ministeri, enti, etc.) per dotare gli utenti comunali di percorsi protetti e riservati.

Nonostante le potenzialità tecniche dei prodotti hardware e software installati, allo stato attuale le funzioni e le misure protettive su indicate sono applicate e funzionanti solo in parte, e ciò a causa sia della attuale insufficienza dello staff tecnico, che non dispone delle risorse umane necessarie a fronteggiare le numerose attività richieste dalla manutenzione e gestione del sistema, sia per una oggettiva attuale inadeguata preparazione degli utenti alla cultura della ottemperanza alle misure di riservatezza.*(aggiunta)*

Per rendere operative, efficaci e stabili nel tempo le misure di protezione e di riservatezza dei dati, si rileva pertanto l'opportunità della formulazione e della messa in atto di un piano complessivo, mirante sia alla costituzione di un nucleo di assistenza agli utenti e di gestione del Sistema Informativo nella sua generale applicazione, sia alla formazione degli utenti in relazione alla privacy.

In conclusione, con la formulazione del presente Documento Programmatico della Sicurezza si ravvisa l'opportunità della definizione

² applicabile solo in presenza dei Sistemi Operativi Microsoft Windows 2000 e XP

e l'avvio di un piano generale di riqualificazione del Sistema Informativo Comunale, articolato secondo i capoversi seguenti:

- A. Riconversione dell'Hardware mediante acquisto di unità tecnologicamente aggiornate;
- B. Costituzione di uno staff tecnico adeguato per tutte le operazioni di assistenza agli utenti, di gestione e manutenzione delle procedure;
- C. Formulazione di un calendario di incontri di formazione per gli addetti all'impiego delle procedure e al trattamento dei dati comunali.

Nell'insieme del piano di riconversione, il punto C assume una posizione di particolare rilevanza. Infatti per la peculiare caratteristica delle attività comunali, una determinata operazione contenente dati riservati, per quanto la si possa definire originatesi o di pertinenza di una specifica area (ad es. : il personale), per le esigenze procedurali dovrà transitare per aree diverse, quali gli Affari generali - per la compilazione di delibere o di atti consimili - e della Ragioneria - per la collocazione in bilancio e la formazione di mandati. E quindi, per quanto il dato sia protetto e custodito negli archivi di competenza, non si può evitare che durante le vicissitudini dello sviluppo di una pratica, esso si trovi esposto al transito e quindi a rischi di fortuita o illecita diffusione nelle diverse aree di competenza che incontrerà nel suo percorso procedurale. Il contenimento di tale rischio di trattamento improprio, dovuto dunque alle peculiari caratteristiche di "trasversalità" delle procedure comunali, piuttosto che alle proprietà tecnologiche del sistema, risulta affidato alla preparazione degli addetti, e quindi dipendente dal fattore umano, che è proprio quello curato nel punto C del piano di riqualificazione.

*Paragrafo 3 – Elenco delle Banche Dati e delle Applicazioni contenenti
Dati Personali*

Nel presente paragrafo sono elencati gli archivi di competenza per ciascuna delle macro aree di attività comunali. La tabella a seguito illustrata va compilata a cura del Dirigente Responsabile di ciascuna Area.

----- *fac-simile di modulo* -----

Documento Programmatico sulla Sicurezza

Tabella 1

Dichiarazione Banche Dati

in carico alla struttura.....

Il sottoscritto

in qualità di dirigente Responsabile della struttura

dichiara che la propria struttura organizzativa detiene e gestisce i
seguenti archivi:

| <i>Denominazione dell'Archivio</i> | <i>Contenuti – destinazione d'uso e impieghi</i> | <i>in forma elettronica</i> | <i>in forma cartacea</i> |
|--|--|---------------------------------|------------------------------|
| | | | |
| | | | |
| | | | |

Il Dirigente Responsabile

(timbro e firma)

----- *(da allegarsi al presente documento programmatico)* -----

Paragrafo 4 – Interventi prioritari sul Sistema Informativo

Nel quadro del piano di riqualificazione del Sistema informativo, con particolare riferimento alle Misure Minime di Sicurezza riportate agli Artt. 34 e 35 del Dlg. 196 del 30 giugno 2003, in attuazione a quanto illustrato al Paragrafo 3 del presente Documento programmatico, si decide di dare priorità massima ai seguenti interventi:

sostituzione dei PC di non recente produzione, dotati di Sistema Operativo e di File System³ non adatti alla gestione delle password;

sostituzione delle attuali password di accesso con un nuovo sistema di Password da 8 posizioni alfanumeriche, periodicamente rinnovate, secondo le indicazioni di Legge;

costituzione di un registro delle autenticazioni, con date di decorrenza e di scadenza delle stesse, e dei relativi rinnovi.

programmazione di un ciclo di corsi sulla privacy e sulle procedure di sicurezza rivolto a tutti i dipendenti comunali – con particolare attenzione verso i reparti in cui i dati personali e sensibili vengono gestiti;

programmazione di un ciclo di incontri con i dirigenti responsabili della custodia e del trattamento dei dati sensibili, per la disanima e la discussione sulle procedure di gestione dei dati, sulla disciplina degli accessi agli ambienti comunali, e sull'osservanza delle procedure di sicurezza nei rapporti con il pubblico;

costituzione di una struttura operativa EDP, di assistenza agli utenti e di manutenzione del Sistema Informativo Comunale

³ MsWindows '98; File System FAT invece di NTFS

Paragrafo 5 – I Soggetti del trattamento dei dati

La tabella appresso riportata deve essere compilata a cura dei responsabili di ciascuna area, e deve riportare – per ciascuna banca dati di propria competenza – sia essa in forma cartacea o gestita informaticamente – quali sono gli addetti autorizzati all’accesso dei dati, e incaricati a compiere su di essi le operazioni di lettura, immissione e modifica delle registrazioni.

----- *fac-simile di modulo* -----

Documento Programmatico sulla Sicurezza

Tabella 2

Dichiarazione Incaricati al trattamento dei dati (All.B – regola 19.2)
in carico alla struttura.....

Il sottoscritto

in qualità di Dirigente Responsabile della struttura
dichiara che le Banche Dati di propria competenza sono gestite come segue

| <i>Denominazione dell'Archivio</i> | <i>Autorizzati all'accesso e all'immissione e modifica dei dati</i> | <i>in forma elettronica</i> | <i>in forma cartacea</i> |
|------------------------------------|---|-----------------------------|--------------------------|
| | | | |
| | | | |

Il Dirigente Responsabile

(timbro e firma)

----- *(da allegarsi al presente documento programmatico)* -----

Capitolo II

Analisi dei rischi – misure in essere e da adottare

(ex Dlg.196 30 giugno 2003 - All.B - regole 19.3 – 19.4)

Paragrafo 6 – Contenuti – Enumerazione dei rischi

Nella presente sezione sono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati nel Comune di Campanium, sia in relazione al contesto fisico – ambientale specifico del Comune, sia in relazione agli strumenti utilizzati; se ne valutano le possibili conseguenze, si descrive lo stato delle misure in essere e si riportano, in sintesi programmatica, le misure che si conviene di adottare per contenere e scongiurare i rischi individuati.

In un contesto di elencazione generalizzata, gli eventi potenzialmente dannosi sono così enumerabili:

a – comportamenti degli operatori

1. sottrazione di credenziali di autenticazione
2. inconsapevolezza, disattenzione o incuria
3. comportamenti sleali o fraudolenti
4. errore materiale

b – eventi relativi agli strumenti

1. azione di virus informatici o di programmi suscettibili di recare danno
2. spamming o tecniche di sabotaggio
3. malfunzionamento, indisponibilità o degrado degli strumenti

4. accessi esterni o non autorizzati
5. intercettazione di informazioni in rete
6. malfunzionamenti o inefficienze attribuibili ai programmi applicativi

c – eventi relativi al contesto fisico – ambientale

1. ingressi non autorizzati a locali o aree ad accesso ristretto
2. sottrazione di strumenti contenenti dati
3. eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria
4. guasti a sistemi complementari (impianto elettrico, idrico, climatizzazione, etc.
5. Degrado e abbandono
6. errori umani nella gestione della sicurezza fisica

Nella specifica situazione del Comune di Campanium - nella premessa che l'attenta vigilanza prestata ad ogni livello e il senso di consapevolezza e di responsabilità prodigate da ognuno degli addetti comunali sono tali da configurare un ambiente di norma sufficientemente protetto dagli eventi dannosi di qualsiasi natura - si stima che le situazioni pericolose potenzialmente più probabili siano da annoverarsi tra le seguenti:

lettera a – punti 2 e 4

la ripetitività di alcune operazioni e procedure può portare a disattenzioni e errori incidentali;

lettera b – tutti i capoversi

situazioni di vulnerabilità possono essere individuate sia nello stato di carente manutenzione delle apparecchiature (punto 3), sia nella non ottemperanza alle norme di sicurezza e di disciplina nelle comunicazioni digitalizzate da e verso l'esterno (punti 1, 2, 4, 5);

lettera c;

Punto 1 - Ci si riferisce alla consueta accessibilità ai locali del Comune. In essi vengono trattati dati e documenti di carattere riservato e sensibile, e tuttavia si annoverano talvolta situazioni in cui i locali sono – anche per brevi intervalli – lasciati incustoditi, con documenti disposti sui ripiani e i computer aperti. Ciò avviene in particolare negli intervalli e al di fuori degli orari di lavoro, quando anche elementi esterni possono aggirarsi nell'interno dell'edificio comunale e introdursi senza ostacoli di sorta negli ambienti più disparati.

Il punto 3 merita una particolare attenzione, perché esso trova riferimento nella necessità di proteggere gli archivi elettronici dei dati comunali da ogni possibile disastro, sia esso di natura dolosa, sia accidentale o dovuto a calamità naturali. Nell'epoca attuale sempre più ci si rende conto che, per la complessità e la multiformità dei rapporti tra stato, enti locali e cittadini, è estremamente importante mantenere un archivio accurato di tutti gli accadimenti che abbiano rilevanza giuridica. Deve pertanto essere posta in atto ogni possibile misura per proteggere l'integrità degli archivi che contengono gli atti custoditi dal Comune, perché in essi risiede non solo la memoria dei doveri, ma soprattutto le garanzie civili dei cittadini.

Per ciò che attiene al punto 5 – degrado e abbandono – il Comune di Campanium è consapevole del deplorabile stato in cui versa una parte antica ma non per questo meno preziosa del proprio archivio della

cittadinanza, che è quella concernente le incomparabili registrazioni originali degli Atti Pubblici dei cittadini di Campanium del 19-esimo secolo. Sull'intervento da adottare in proposito un capoverso è dedicato nel paragrafo successivo.

Paragrafo 7 - Misure da adottare

Per quanto nessuno degli eventi potenzialmente dannosi sia da escludersi aprioristicamente, il Comune di Campanium individua la necessità di interventi mirati specificamente nei punti su esposti, e pertanto per essi dispone ed elenca nel presente paragrafo con opportuno rilievo le norme comportamentali e organizzative di prevenzione e di contenimento da attuare in tempi brevi e mediante piani di attuazione specifici da definirsi:

a - Comportamenti degli operatori

Il Comune ravvisa nell'introduzione delle norme di sicurezza definite nel Dlg. 196 l'opportunità di rammentare – sotto forma di apposite riunioni e seminari – agli addetti di ogni area di attività – quali sono i comportamenti e le attenzioni specifiche da prestare nel trattamento dei dati personali, sensibili e giudiziari, sia in ordine alla protezione e alla sicurezza dei dati stessi, dei quali il Comune è totalmente responsabile, sia nei riguardi del comportamento e del rispetto dovuto ai cittadini interessati e a coloro che fanno richiesta dei servizi comunali; pertanto i Dirigenti Responsabili di ogni area sono sensibilizzati a concepire e mettere in atto le iniziative che riterranno più idonee per informare e sensibilizzare adeguatamente i propri collaboratori al riguardo, senza trascurare gli aspetti di responsabilità civile e penale che la Legge 196

richiama esplicitamente in ordine ai comportamenti illeciti e lesivi della sicurezza dei dati.

Particolare menzione merita l'aspetto relativo ai normali rapporti di collaborazione che legano il Comune di Campanium ad altri Enti Pubblici ad esso collegati. In virtù dei suddetti rapporti addetti e funzionari di Enti esterni, quali ad esempio Acquedotto, Polizia, Carabinieri, Regione, Aziende private accreditate etc. chiedono ed ottengono la collaborazione del Comune per ciò che concerne ricerche di documenti, cittadini, situazioni, etc., intervenendo direttamente – e talvolta in piena indipendenza - sugli archivi del Comune.

Pur apprezzando tutti gli aspetti che detta collaborazione comporta, il Comune di Campanium esprime preoccupazione che attraverso gli aspetti logistici di questi momenti di collaborazione vengano inconsapevolmente violati i diritti di riservatezza dei cittadini nonché la sicurezza e l'integrità degli archivi; e pertanto invita il Dirigente Responsabile degli Archivi Anagrafici a vigilare sugli aspetti descritti, e disporre che in ogni caso gli interventi di collaborazione si svolgano sotto il controllo diretto di un rappresentante del Comune, siano accuratamente e dettagliatamente documentati con apposita modulistica, oltre che debitamente sottoscritti dai rappresentanti dell'Ente che ha fatto richiesta ed ottenuto la collaborazione medesima.

b - Eventi relativi agli strumenti

Per ciò che attiene al malfunzionamento, all'indisponibilità e al degrado degli strumenti – eventi questi che il Comune di Campanium riconosce come particolarmente pericolosi ai fini della sicurezza e alla protezione di dati – si dispone che il Responsabile dei Servizi Informatici del Comune verifichi che sia operativo un adeguato contratto di assistenza e di manutenzione agli strumenti, alla rete e ai sistemi operativi di base; e verifichi inoltre che la ditta contraente risponda alle esigenze del

comune di Campanium sia per ciò che attiene alla prontezza e all'efficacia degli interventi, sia per le garanzie in ordine all'applicazione delle norme di sicurezza e protezione dei dati, prescritte dalla legge 196 nei riguardi delle ditte esterne che mantengono con il Comune rapporti di servizio in out-sourcing.

In merito poi agli eventi dannosi provocati dai virus informatici, dai programmi di "spamming" e alle altre tecniche di sabotaggio e di intercettazione che tendono ad infiltrarsi nella rete comunale dell'esterno, si richiede al responsabile dei servizi informativi e del Ced nel suo complesso di attuare e sorvegliare che siano installati e funzionanti a monte della rete gli opportuni strumenti hardware e software atti a far diga e respingere gli attacchi informatici suddetti; ma contemporaneamente – e ciò a specifico richiamo agli accessi a- e dall'esterno non autorizzati, il Comune di Campanium raccomanda e dispone con fermezza che non siano consentite installazioni di linee di comunicazione dati e connessioni tecnologiche di qualsiasi natura, che non facciano capo a quei dispositivi di controllo centralizzati (software antivirus e dispositivi firewall) installati, configurati e tenuti in stato di efficienza a cura e sotto il diretto controllo del Responsabile dei Servizi Informatici. Ciò vuol dire anche che si dispone vengano immediatamente rimosse tutte le connessioni analogiche o digitali che siano attualmente attive tramite modem o Line Adapter direttamente collegati a PC comunali. Le uniche connessioni con l'esterno ammesse saranno da ora in avanti soltanto quelle approvate, istituzionalizzate e direttamente monitorate dal Centro Elaborazione Dati.

Infine, con riferimento al Sistema dei Programmi Applicativi – benchè sia tuttora attivo il rapporto contrattuale con la ditta incaricata della fornitura e dell'installazione del Sistema Informativo per ciò che attiene ad interventi su eventuali malfunzionamenti – non risulta che sia stato

tuttora provveduto alla installazione di un sistema gerarchico di accessi che disciplini i livelli e le specifiche funzionali di autorizzazione degli utenti autenticati. A causa di ciò la sicurezza e la protezione dei dati risulta compromessa perchè gli accessi ai dati sono ripartiti tra gli addetti ai servizi senza che sia definita un'adeguata distribuzione delle funzioni e delle responsabilità.

c - Eventi relativi al contesto fisico – ambientale

Si individuano nei punti 1 e 3 gli eventi più suscettibili di arrecare danno alla sicurezza dei dati Comunali. Particolare menzione merita inoltre il riferimento al punto 5.

Il punto 1 si riferisce agli accessi non autorizzati a locali ed aree ad accesso ristretto. Si dispone a tal proposito che i Dirigenti Responsabili di area dispongano e sorveglino che i documenti e i dossier contenenti i dati siano sempre tenuti negli appositi armadi sotto chiave, e che i locali stessi siano lasciati chiusi, anche nel caso di assenza soltanto temporanea degli addetti. Durante l'accesso agli addetti di Imprese esterne incaricate di interventi di manutenzione, la sicurezza e la protezione dei dati verrà affidata a dipendenti comunali appositamente incaricati della sorveglianza.

Per ciò che attiene al punto 3, al fine di un'adeguata protezione dei Sistemi Server, in cui i dati Comunali vengono trattati, si raccomanda che l'ambiente venga attrezzato da un sistema anti incendio e che i nastri contenenti le copie di salvataggio dei dati vengano custoditi in un armadio ignifugo. Ed inoltre, a conclusione della disamina sulla sicurezza degli archivi, e con riferimento ai criteri e alle modalità di ripristino della disponibilità dei dati (All. B – regola 19.5), allo scopo

di mantenere costantemente sotto controllo l'efficienza e la piena funzionalità delle procedure Comunali, si invita il Dirigente Responsabile del Sistema Informativo a disporre e curare che sia messo a punto, e tenuto pronto per ogni evenienza, un piano di intervento rapido in grado di ripristinare in poche ore il Sistema anche nel caso di completa distruzione dei Server con perdita dei dati in essi contenuti.

In merito al punto 5 – stato di abbandono dell'archivio storico della cittadinanza – il Comune invita il Dirigente Responsabile a predisporre in breve tempo una relazione sullo stato attuale – igienico e organizzativo - degli archivi, sulla accessibilità degli stessi, sulla sicurezza e illuminazione delle scale e dei corridoi di accesso, sulle precauzioni anti-incendio e anti effrazione disposte e sulla loro efficienza, sulla disponibilità e proprietà degli spazi e dei supporti per la custodia e della protezione dei registri, ed infine chiede che venga predisposto un adeguato piano di ripristino che riporti la protezione dei dati dell'archivio storico nella norma e nella sicurezza – intendendosi per essa sia la sicurezza dei dati⁴ sia la sicurezza stessa degli addetti che hanno in custodia questo importante e significativo elemento della memoria della città di Campanium.

Paragrafo 8 – Documentazione sui Rischi e sugli interventi suggeriti

Gli aspetti ambientali e strumentali degli eventi potenzialmente dannosi, nonché quelli specificamente legati alle interrelazioni tra l'ambiente e gli addetti comunali e i cittadini sono molteplici e spesso difficilmente percepibili per chi esamina dall'esterno tale problematica. Per questa ragione è particolarmente preziosa e significativa la testimonianza che – pur nella necessaria schematicità – è possibile raccogliere attraverso la

⁴ Si prenda in considerazione la riproduzione digitale dei documenti più significativi

tabella a seguito delineata. Il Dirigente Responsabile interverrà sulla compilazione della tabella in oggetto curando che cenni seppur essenziali vengano inseriti a segnalazione delle più stringenti e improcrastinabili necessità di intervento.

----- *fac-simile di modulo* -----

Documento Programmatico sulla Sicurezza

Tabella 3

Dichiarazione dei rischi incombenti sui dati (All.B – regola 19.3)
in relazione alla struttura.....

Il sottoscritto

in qualità di Dirigente Responsabile della struttura

dichiara che gli eventi potenzialmente dannosi cui sono esposti i dati nella struttura di sua competenza sono elencati nella tabella seguente:

| <i>Definizione dell'Evento potenzialmente dannoso</i> | <i>Archivi e Documenti esposti all'evento dannoso</i> | <i>suggerimenti sui possibili rimedi</i> |
|---|---|--|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Il Dirigente Responsabile

(timbro e firma)

----- (da allegarsi al presente documento programmatico) -----

Capitolo III

Pianificazione degli Interventi Formativi

(ex Dlg.196 30 giugno 2003 - All.B - regole 19.6)

Paragrafo 9 – Contenuti

In punti diversi del presente documento si è sottolineata l'importanza di un adeguato piano di formazione, perché esso costituisce – è comune convincimento – l'elemento indispensabile per il coinvolgimento degli addetti comunali, a qualsiasi livello. E' tuttavia fondamentale che detto piano non sia presentato e assolto come un adempimento fine a se stesso, esprimendosi in riunioni in cui vengano sterilmente elencati i vincoli e i comportamenti prescritti dalla legge; ma che piuttosto sia il momento di sintesi - di "istruzioni per l'uso" - di quelle revisioni e quei riadeguamenti di procedure e di strutture, strumentali e di ambiente, che la legge 196 ha ispirato e che il Comune di Campanium ha deciso di porre in atto.

Pertanto saranno accolte con interesse e preminente considerazione le proposte di adeguamento culturale e comportamentale che saranno suggerite dai Responsabili di Area, con la certezza che le suddette iniziative renderanno comprensibili, bene accette e di agevole applicazione, le revisioni che la protezione e la sicurezza dei dati avranno rese necessarie.

Come risultato degli interventi formativi summenzionati, ci si attende che rinnovato rispetto e considerazione verrà rivolto alle esigenze dei cittadini, che la più attenta cura sarà tributata alla custodia dei documenti e delle pratiche d'ufficio, che alle procedure informatiche più

complesse vengano prestate attenzione, competenza, tenacia e flessibilità.

I Dirigenti d'Area sono invitati ad indagare e riflettere, con l'aiuto dei più stretti collaboratori, sugli interventi formativi che meglio si attagliano alle strutture di loro riferimento, e sui temi più emergenti che, trattati organicamente in sessioni di studio collettive, maggiormente possono recare giovamento alla produttività dei reparti. Il risultato di tali indagini e riflessioni potrà trovare posto nella tabella seguente:

----- *fac-simile di modulo* -----

Documento Programmatico sulla Sicurezza

Tabella 4

Dichiarazione sugli interventi formativi (All.B – regola 19.6)
in relazione alla struttura.....

Il sottoscritto

in qualità di Dirigente Responsabile della struttura
sottopone all'attenzione l'efficacia degli interventi formativi a seguito suggeriti

| <i>Descrizione sintetica dell'intervento formativo</i> | <i>Modalità dell'intervento formativo</i> | <i>Classi omogenee cui l'intervento è destinato</i> |
|--|---|---|
| | | |
| | | |
| | | |

Il Dirigente Responsabile

(timbro e firma)

----- *(da allegarsi al presente documento programmatico)* -----

Capitolo IV
Trattamenti affidati all'esterno
(ex Dlg.196 30 giugno 2003 - All.B - regola 19.7)

Paragrafo 10 – Inventario e controllo dei trattamenti

Nel presente capitolo il Comune di Campanium ravvisa – per la completezza dell'applicazione della legge 196 – la necessità di esercitare un attento controllo sulle attività affidate all'esterno che comportano il trattamento di dati personali e sensibili. Numerosi sono infatti i servizi che richiedono gli affidamenti a terzi di dati personali, e conseguentemente elevato è il rischio che in tali circostanze il dato “esternalizzato” venga adoperato o diffuso in modo improprio, con conseguentemente grave compromissione del Comune.

Consapevoli del fatto che è possibile esercitare un controllo sui dati solo fintanto che essi si trovano sotto il controllo diretto del Comune, e che non v'è rimedio alcuno quando i dati affidati all'esterno vengono utilizzati indebitamente, è indispensabile che le ditte affidatarie siano in grado di offrire convincenti credenziali in ordine alla riservatezza dei dati.

A tal fine ogni Dirigente Responsabile d'Area opererà un'attenta revisione dei rapporti in oggetto, e provvederà alla compilazione particolareggiata ed esaustiva della natura dei rapporti che l'area di sua competenza intrattiene con enti esterni, pubblici o privati, per qualsiasi servizio o ottemperanza di legge. La tabella da compilare è illustrata nella pagina seguente:

----- *fac-simile di modulo* -----

Documento Programmatico sulla Sicurezza

Tabella 5

Dichiarazione sui trattamenti affidati all'esterno (All.B – regola 19.6)
in relazione alla struttura.....

Il sottoscritto

in qualità di Dirigente Responsabile della struttura

elenca qui di seguito il quadro completo delle attività affidate a terzi, sia nell'ambito degli ambienti comunali, sia all'esterno:

| <i>Descrizione dell'attività esternalizzata</i> | <i>Trattamenti di dati effettuati nell'ambito dell'attività</i> | <i>Società, Ente o Consulente cui è affidata l'attività - e ruolo ricoperto agli effetti della disciplina sulla protezione dei dati⁵</i> |
|---|---|---|
| | | |
| | | |
| | | |

Il Dirigente Responsabile

(timbro e firma)

----- (da allegarsi al presente documento programmatico) -----

⁵ Nominativo del Titolare o Responsabile del trattamento dei dati

Paragrafo 11 – Conclusione

La presente relazione costituisce il Documento Programmatico sulla Sicurezza del Comune di Campanium. Redatto e approvato nel mese di Gennaio del 2005, esso rappresenta in molte sue parti proposte e intenti, più che risultati organizzativi.

Tuttavia il Comune di Campanium - consapevole della scelta di cultura e rispetto civile rappresentati nello spirito e nella lettera della Legge 196/2003 – sottolinea con questo primo rilascio del Documento Programmatico il suo proposito di perseguire l’ottemperanza alle disposizioni della Legge 196 in un percorso di risultati progressivi – nel quadro delle disponibilità del bilancio e dell’impegno dei propri quadri dirigenti.

Campanium, 27 gennaio 2005