



COMUNE DI CITTA' DI CASTELLO

Provincia di Perugia

ALLEGATO I

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI (Artt. 33 – 34 – 35 - 36 e punto 19 allegato B del D.lgs. 196/2003)

DICEMBRE 2005

SOMMARIO

1. INTRODUZIONE	3
2. INDIVIDUAZIONE DEGLI ELEMENTI PER LA REDAZIONE DEL DPS	5
3. PIANI FORMATIVI	6
4. TABELLE UTILIZZATE PER LA DEFINIZIONE DEL DPS.....	7
4.1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI (REGOLA 19.1), DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI (REGOLA 19.2), EVENTUALI TRATTAMENTI AFFIDATI ALL'ESTERNO (REGOLA 19.7)	7
4.2. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (REGOLA 19.3)	7
4.3. MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITÀ DEI DATI, NONCHÉ LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITÀ (REGOLA 19.4)	9
4.4. MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI (REGOLA 19.5)	12
4.5. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI (REGOLA 19.6).....	13

1. INTRODUZIONE

Il presente documento è redatto sulla base delle “Disposizioni inerenti l’adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dagli articoli 33 – 34 – 35 – 36 e dall’Allegato B del D.lgs. 196/2003”.

Le citate disposizioni impongono la predisposizione e l’aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno), di un Documento Programmatico sulla Sicurezza dei dati, per definire, sulla base dell’analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell’ambito delle strutture preposte al trattamento dei dati stessi, i seguenti elementi:

1. l’elenco dei trattamenti dati personali
2. la distribuzione dei compiti e delle responsabilità nell’ambito delle strutture preposte al trattamento dei dati
3. l’analisi dei rischi che incombono sui dati
4. le misure da adottare per garantire l’integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell’ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali
7. la descrizione dei criteri da adottare per garantire l’adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all’esterno della struttura del titolare
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l’individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell’interessato.

Tale documento deve essere obbligatoriamente predisposto nel caso di trattamenti di dati sensibili o giudiziari. Questo è il caso di una Pubblica Amministrazione quale è il Comune di Città di Castello, che tratta, per le incombenze di legge ed i servizi istituiti in favore della cittadinanza amministrata, una molteplicità di dati, fra cui sicuramente dati definiti dalla normativa “sensibili”.

In alcuni casi particolari il Comune si trova, inoltre, a dover gestire anche dati definiti dalla legge “giudiziari”.

Il presente documento darà conto delle misure adottate in relazione alla tipologia delle varie banche dati.

Il presente documento verrà redatto in base alle seguenti sezioni:

1. censimento di tutti i trattamenti effettuati e delle banche dati costituite presso gli uffici comunali
2. analisi dei rischi connessi alla gestione delle banche dati
3. indicazione di un piano delle principali misure di controllo necessarie per ciascun rischio individuato
4. indicazioni i ripristino per ognuna delle banche dati
5. programma di informazione e formazione di tutti i soggetti interessati

2. INDIVIDUAZIONE DEGLI ELEMENTI PER LA REDAZIONE DEL DPS

Mediante la Scheda di rilevazione dei trattamenti, sono state censite, da tutti i Dirigenti di Servizio operanti nei vari uffici dell'Ente, le varie banche dati esistenti. Attraverso tale censimento è possibile ricavare l'elenco dei vari trattamenti di dati in essere e la loro relazione con le stesse banche dati.

La modulistica consente anche di ottenere, per ciascuna banca dati rilevata, informazioni circa

1. il trattamento per il quale viene impiegata
2. la tipologia dei dati trattati
3. i soggetti ai quali i dati si riferiscono
4. le operazioni di trattamento eseguite su di esse
5. le modalità di trattamento dei dati
6. la normativa di riferimento dalla quale discende la necessità della costituzione della banca dati stessa
7. le eventuali comunicazioni dei dati ad altri soggetti
8. l'eventuale diffusione dei dati
9. l'eventuale intervento di terzi nella manipolazione della banca dati
10. i soggetti coinvolti, a vario titolo, nella manipolazione dei dati contenuti
11. i trattamenti affidati all'esterno dell'Ente

3. PIANI FORMATIVI

Il Documento Programmatico sulla Sicurezza riporta poi le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Si descrivono sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 dell'allegato B del D.lgs. 196 del 2003; si individuano le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza; si indicano poi anche i tempi previsti per lo svolgimento degli interventi formativi.

In questo quadro il D.lgs n. 196 del 2003 ha poi introdotto una nuova regola per rendere meglio edotti gli organi di vertice del titolare del trattamento e responsabilizzarli in materia di sicurezza, attraverso l'obbligo di riferire nella Relazione di accompagnamento di ciascun bilancio di esercizio, circa l'avvenuta redazione o aggiornamento del DPS che sia obbligatorio come "misura minima" o che sia comunque adottato (regola 26 Allegato B).

I dati raccolti, attraverso la Scheda di rilevazione dei trattamenti sono riportati nelle varie tabelle riepilogative riportate nel seguito.

4. TABELLE UTILIZZATE PER LA DEFINIZIONE DEL DPS

4.1. Elenco dei trattamenti di dati personali (regola 19.1), distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (regola 19.2), eventuali trattamenti affidati all'esterno (regola 19.7)

Nelle tabelle, che attualmente sono archiviate presso il Servizio CED, sono riportate per ogni trattamento sia le informazioni di base, che le strutture preposte allo specifico trattamento con la ripartizione delle competenze, nonché gli eventuali soggetti esterni che concorrono al trattamento.

Non sono riportate tutte le informazioni rilevate con le schede, ma solo quelle strettamente necessarie per redazione del D.P.S..

4.2. Analisi dei rischi che incombono sui dati (regola 19.3)

I rischi che incombono sulle banche dati, centralizzate o meno, sono riassunti nella tabella di seguito riportata.

Evento	Impatto sulla sicurezza
E1. Sottrazione di credenziali di autenticazione.	Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può in principio sapere dell'occorrenza di tale furto.
E2. Errore materiale	A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli addetti al trattamento possono compiere operazioni errate o specificare dati errati. Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.
E3. Comportamenti illegali	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
E4. Comportamenti sleali e/o fraudolenti	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di

	dati.
E5. Virus informatici	Nel sistema in cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può venirsi ad installare o essere semplicemente eseguito del software spurio del tipo "virus" informatico. Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
E6. Spamming	Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta spuria generata anche con strumenti automatizzati. Tali messaggi possono contenere false notizie. Gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non regolari.
E7. Malfunzionamento apparecchiature	I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da cui possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare. Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati.
E8. Degrado apparecchiature	I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono essere soggetti a degrado naturale conseguente all'uso o al solo funzionamento. Da ciò possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.
E9. Accesso non autorizzato a locali da cui si può accedere ai dati	Un soggetto autorizzato allo scopo, può comunque accedere fisicamente ai locali e manipolare la banca dati esistente. Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.
E10. Eventi distruttivi	I sistemi HW/SW e/o i supporti di

naturali/artificiali accidentali o volontari	memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono essere interessati da eventi distruttivi di origine sia fortuita che dolosa. Dall'evento può derivare la distruzione totale o parziale della banca dati.
--	---

4.3. Misure da adottare per garantire l'integrità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità (regola 19.4)

Gestione credenziali

Fa fronte all'evento E1. Sottrazione di credenziali di autenticazione

Le credenziali di autenticazione dei server sono conosciute solo agli addetti CED, non sono comunicate ad altri soggetti e sono variate con cadenza trimestrale o quando se ne ravvisi la necessità.

Le credenziali di autenticazione di ogni singolo Personal Computer sono conosciute solo agli utenti che operano sullo stesso. Ogni utente ha una propria configurazione con relativa credenziale di accesso.

Per quanto riguarda gli accessi alle banche dati, gli utenti che operano sulle stesse in inserimento, modifica e cancellazione sono dotate di credenziali personali: un unico utente con relativa password esiste per la visualizzazione di alcune informazioni relative ai dati anagrafici.

Gestione dei backup

Fa fronte a tutti gli eventi E1. Sottrazione di credenziali di autenticazione, E2. Errore materiale, E3. Comportamenti illegali, E4. Comportamenti sleali e/o fraudolenti, E5. Virus informatici, E6. Spamming, E7. Malfunzionamento apparecchiature, E8. Degrado apparecchiature, E9. Accesso non autorizzato a locali da cui si può accedere ai dati, E10. Eventi distruttivi naturali/artificiali accidentali o volontari.

Per far fronte a tutti i rischi, sono indispensabili, infatti una corretta gestione dei backup, nonché una corretta conservazione dei supporti su cui sono archiviati gli stessi.

Si riporta di seguito, nella tabella A, l'elenco delle banche dati centralizzate ed i nomi dei rispettivi server che le ospitano.

Tabella A

Nome Server	Sistema Operativo	Data Base	Banca Dati
Cast1	Unix	Informix	Aeraria (Contabilità prima di e-Serfin) CSIO (Stipendi prima di Zucchetti) Duplicazione Demos (Demografica)
Cast2	Unix	Informix	Demos (Demografica)
Flash	Windows NT4	Oracle	e-Serfin (Contabilità) e-Trib (Tributi) Concilia (Multe) Tradewin (Commercio)
Urano	Windows 2000	Access	PRG (Consultazione in Internet del Piano Regolatore Generale) Azimut (Protezione Civile)
Hypnos	Windows 2000	Lotus Notes	Si.Ge.D (Protocollo, Delibere, Atti)
Argo	Windows 2003	SQL Server	Sosia (Ristorazione scolastica) Gradus (Graduatorie nidi) Zucchetti (Paghe)
			Programmi realizzati dal CED

Sono presenti presso la sala macchine del CED altri server che riportiamo di seguito nella Tabella B perché sono richiamati in altre parti del documento.

Tabella B

Nome Server	Sistema Operativo	Banca Dati
NT1	Windows NT4	Dominio principale Posta interna Stampanti di rete
Intgw	Windows NT4	Dominio di backup Proxy Internet
Aracne	Windows 2000	Pubblicazione sito Posta esterna
Argo	Windows 2003	Application Server per le procedure che sono in Terminal Server
Nas1	Windows 2000 server	Backup Nas Server (Cartelle condivise)
Atena	Windows 2003 server	Gestione Antivirus Backup per procedure in SQL Server

Il salvataggio delle banche dati centralizzate residenti nei server è in carico al CED.

Le banche dati residenti nei server vengono salvate quotidianamente, a partire dalle ore 1.00 di notte, allo scopo di fornire almeno una versione aggiornata alla notte precedente: le banche dati delle procedure e-Serfin, e-Trib, Concilia, Tradewin, Si.Ge.D., Sosia, Gradus e Zucchetti vengono inoltre salvate anche nel server Nas1.

Le copie vengono effettuate su cassette a nastro magnetico ad alta capacità e riposte in una cassaforte ignifuga posta in altro locale distante dai locali del CED (locale Messi Comunali a piano terra).

Le copie giornaliere vengono ricoperte ogni quindici giorni, le mensili ogni 4 mesi: vengono conservate per tre anni le copie al 31.12 di ogni anno.

Prima di ogni aggiornamento delle procedure centralizzate a versioni successive viene effettuato un salvataggio ulteriore della procedura in questione che viene conservato per un mese.

Ogni lunedì o primo giorno utile della settimana viene controllato dall'incaricato dei salvataggi dei dati la correttezza degli stessi.

Anche tutte le cartelle e le sotto-cartelle condivise, di ogni Settore e/o Servizio, residenti nel server Nas1, vengono salvate giornalmente. I salvataggi di dette cartelle seguono lo stesso ciclo dei salvataggi delle banche dati che risiedono nei server della Tabella A.

Per le banche dati non centralizzate, ma residenti nei singoli Personal Computer sono responsabili dei relativi salvataggi i singoli soggetti; gli stessi sono responsabili anche di una corretta custodia dei supporti magnetici su cui risiedono i singoli backup, in quanto i supporti removibili devono essere riposti in luogo sicuro ed inaccessibile a soggetti estranei.

Protezione delle aree e dei locali

I locali della sala macchine del CED sono accessibili solo agli addetti del CED che ne detengono le chiavi. Si può accedere a detti locali solo dietro apposito riconoscimento del soggetto che ne richiede l'accesso.

Qualora sia necessario un intervento tecnico o un intervento di assistenza su una procedura residente in uno dei server da una ditta esterna, l'intervento viene effettuato in presenza di uno degli addetti che vigila e ne controlla le attività.

Lo stesso modo di procedere si ha anche se gli interventi vengono svolti presso un singolo Personal Computer.

Nella sala macchine è predisposto un impianto elettrico apposito ed un moderno impianto di climatizzazione.

Accanto alla porta di ingresso del CED è collocato un estintore.

I singoli Personal Computer sono ovviamente dislocati in locali normalmente adibiti ad ufficio in cui lavorano i singoli incaricati del trattamento.

Tutti gli uffici, in caso di assenza degli incaricati, vengono chiusi a chiave.

In alcuni casi, sono presenti nei singoli uffici, armadi chiusi a chiave in cui vengono conservati, oltre a documenti cartacei, anche supporti magnetici contenenti i vari backup.

Nel corso della rilevazione dei trattamenti, alcuni locali, soprattutto quelli posti a piano terra, sono risultati ad alto rischio per possibili furti in quanto i locali sono facilmente accessibili da finestre e/o porte a vetri.

Sono esposti a questo rischio

- gli uffici della Polizia Municipale e dell'ufficio Sport siti a piano terra presso la sede di Piazza Garibaldi
- l'ufficio del Centro Documentazione Infanzia (C.D.I.) sito a piano terra della sede di Piazza Le Grazie
- gli uffici dello Sportello del Cittadino (U.R.P.) siti a piano terra presso la sede di Via Cavour
- gli uffici dei Servizi Sociali siti a piano terra presso la sede denominata ex-C.G.I.L.
- gli uffici del cosiddetto Magazzino siti presso la sede di Via Mascagni

Verrà attivato il Settore Tecnico del Comune al fine di pianificare interventi quali la sistemazione di inferriate a porte e/o finestre. Si richiederà che i locali più a rischio siano messi in sicurezza quanto prima.

4.4. Modalità di ripristino della disponibilità dei dati (regola 19.5)

Nel caso delle banche dati centralizzate sono responsabili del ripristino delle stesse gli addetti del CED per quelle banche dati gestite esclusivamente dal CED e per i dati contenuti nelle cartelle e sotto-cartelle dei vari settori/servizi salvati nel server NAS1.

Per le altre banche dati le fasi di ripristino sono gestite congiuntamente con la ditta che svolge assistenza e manutenzione sulla stessa sulle particolari procedure.

Non sono pianificate prove di ripristino.

Per quanto riguarda le banche dati distribuite nei vari Personal Computer, queste vengono ripristinate dai singoli utenti qualora ne ricorra la necessità.

Anche in questo caso non sono pianificate prove di ripristino.

4.5. Pianificazione degli interventi formativi (regola 19.6)

Corso di formazione	Descrizione	Date corsi
<p>La privacy e il regime di trattamento di dati personali nella P.A. (dalla legge 675/96 al D.lgs.196/03)</p> <p>Esempi di particolari trattamenti</p>	<p>Analisi del contesto normativo e approfondimento del D.lgs 196/03. I corsi sono finalizzati a istruire i destinatari su: i rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e quindi sulle modalità per aggiornarsi alle misure minime adottate dal titolare.</p> <p>I corsi si rivolgono ai Responsabili per il trattamento dei dati ed agli Incaricati del trattamento con percorsi specifici legati alle suddette figure presenti nell'Ente.</p> <p>Verrà poi differenziata la formazione</p> <ol style="list-style-type: none"> 1. per gli incaricati che operano nel servizio informativo (CED) vista la particolare rilevanza dei dati trattati 2. per gli incaricati che operano nei Nidi d'Infanzia comunali e convenzionati per la particolarità di dati ed immagini trattati 	<p>1 giorno entro settembre 2006</p> <p>1 giorno entro settembre 2006</p> <p>1 giorno entro settembre 2006</p> <p>1 giorno entro settembre 2006</p> <p>nei vari collettivi che si svolgono nei mesi di settembre e ottobre</p>