CITTÀ DI RAGUSA

DETERMINAZIONE SINDACALE

N. 63 Data 31 MAR. 2008	OGGETTO: Approvazione Documento Programmatico sulla Sicurezza (D.Lgs. n.196/2003 e successive modifiche ed integrazioni).

Dimostrazione della disponibilità dei fondi:

Bilancio 200... Competenze

Capitolo _____spese per_____

Funz._____ Serv._____ Interv._____

Addì _____ IL RAGIONIERE CAPO

.....

Parere del Responsabile del Servizio in merito alla regolarità tecnica:
Si esprime parere FAVOREVOLE

Il Dirigente o responsabile del Servizio

Ragusa, lì 31.3.08 .....

Parere del Responsabile di Ragioneria in merito alla regolarità contabile:
Si esprime parere FAVOREVOLE

Il Responsabile di Ragioneria

Ragusa, lì ....

Per l'assunzione dell'impegno di spesa, si attesta la regolare copertura finanziaria, ai sensi dell'art.55, comma 5°, della legge 08/06/1990, n.142, recepito dalla L.R. n.48/91.

Il Responsabile del Servizio Finanziario

Ragusa, lì ....

Si esprime PARERE FAVOREVOLE all'adozione dell'atto di cui all'oggetto sotto il profilo della sua legittimità.

IL SEGRETARIO GENERALE

Ragusa,lì 31.3.08 .....

CITTÀ DI RAGUSA

IL SINDACO

Premesso che il Decreto Legislativo n. 196/2003 ha previsto l'obbligo per gli enti locali di dotarsi di un documento programmatico sulla sicurezza;

Che di tale incarico il Direttore Generale ha onerato il Dirigente del Settore I;

Che tale incarico ha comportato una serie di attività che sono state svolte nel corso degli anni 2005, 2006, 2007 delle quali si dà atto all'interno del piano che è parte integrante e sostanziale del presente provvedimento;

Che con determinazione sindacale n. 33 del 30/03/2007 è stato approvato il Documento programmatico sulla sicurezza dei dati personali;

Ritenuta la necessità di dovere aggiornar entro la data del 31/03/2008 il citato documento;

Ritenuta la necessità di provvedere in merito trattandosi di una disposizione da eseguirsi tassativamente per disposizione di legge entro la data di scadenza prevista;

Visti i pareri favorevoli espressi dal responsabile in ordine alla regolarità tecnica e il parere di legittimità espresso dal Segretario Generale;

Visto l'art. 41 della L.R. n. 26/93, che attribuisce alla Giunta Municipale la competenza nelle materie indicate nell'art. 15 della L.R. n. 44/91, così consolidandosi l'indirizzo normativo in ordine alla individuazione del Sindaco quale Organo a competenza generale;

Considerato che la materia oggetto del presente provvedimento non rientra tra quelle indicate nel sopraccitato art. 15 della L.R. n. 44/91, per cui il provvedimento stesso rientra nella competenza sindacale;

DETERMINA

1. Approvare l'allegato "Documento Programmatico sulla sicurezza" con relativi allegati, il quale fa parte integrante e sostanziale del presente atto;

2. Dare incarico ai Dirigenti di Settore per l'attuazione delle indicazioni e delle disposizioni in esso previste;

3. Dare atto che il presente provvedimento non comporta impegno di spesa.

IL SINDACO
- Nello Di pasquale -

Parte integrante: Documento Programmatico sulla Sicurezza dei dati personali

Il sottoscritto messo comunale attesta che copia della presente determinazione è stata affissa all'Albo Pretorio il ....09 APR. 2008..... fino al ....23 APR. 2008..... per quindici giorni consecutivi.

Ragusa. lì ....09 APR. 2008.....

IL MESSO COMUNALE
IL MESSO NOTIFICATORE
.....(Licitra Giovanni).....

Certifico che, contestualmente all'affissione all'Albo, la determinazione è stata trasmessa in copia al Presidente del Consiglio, ai sensi del 3° comma dell'art.8 della L.R. n.39/97

Ragusa, lì ....09 APR. 2008.....

IL SEGRETARIO GENERALE
IL FUNZIONARIO C. S.
.....(Giuseppe Tufato).....

Il sottoscritto messo comunale attesta che copia della presente determinazione è rimasta affissa all'Albo Pretorio per quindici giorni consecutivi dal ....09 APR. 2008..... al ....23 APR. 2008.....

Ragusa, lì ....24 APR. 2008.....

IL MESSO COMUNALE
IL MESSO NOTIFICATORE
(Licitra Giovanni)
.....

Certificato di avvenuta pubblicazione della determinazione

Vista l'Attestazione del messo comunale, certifico che la presente determinazione, è stata affissa all'Albo Pretorio di questo Comune il giorno....09 APR. 2008..... ed è rimasta affissa per quindici giorni consecutivi decorrenti dal ....09 APR. 2008..... senza opposizione.

Ragusa, lì ....24 APR. 2008.....

IL SEGRETARIO GENERALE
IL SEGRETARIO GENERALE
Avv. Serafina Buscè
.....

Parte integrante e sostanziale alla Determinazione Sindacale N° 63 del 31-03-2008

CITTÀ DI RAGUSA

www.comune.ragusa.it

SETTORE I – ASSISTENZA AGLI ORGANI ISTITUZIONALI, AFFARI GENERALI
SERVIZI DEMOGRAFICI, STATISTICA, RILEVAZIONI, CENSIMENTI
C.so Italia, 72 – Tel. – Fax 0932 676259 - 676255 - E-mail affari.generali@comune.ragusa.it

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

TITOLARE : COMUNE DI RAGUSA

Data di realizzazione : 31 marzo 2008

DOCUMENTO APPROVATO CON DETERMINAZIONE SINDACALE N. ..... DEL .....

INDICE GENERALE

PARTE III
PIANO DI INFORMAZIONE E FORMAZIONE

CAPITOLO 5

DISAMINA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO

5.1 SCOPO DELLA FORMAZIONE

5.2 TECNICHE E STRUMENTI DI FORMAZIONE DEGLI INCARICATDELTRATTAMENTO DEI DATI PERSONALI

5.3. CONTENUTO DEL PIANO DI FORMAZIONE

5.4. VALUTAZIONE DELL'EFFICIENZA DEL PIANO DI FORMAZIONE

5.5. AGGIORNAMENTO E PROGRAMMI INDIVIDUALI

PARTE IV
ADOZIONE DI MISURE SUPPLEMENTARI E PERIODICI CONTROLLI

CAPITOLO 6

DESCRIZIONE DELLE MISURE E DEI CRITERI DI INTERVENTO IN CASO DI TRATTAMENTI DI DATI PERSONALI AFFIDATI A STRUTTURE ESTERNE (OUTSOURCING)

6.1 SCOPO E LISTA DI CONTROLLO DELLE STRUTTURE ESTERNE

CAPITOLO 7

MISURE DI SICUREZZA SUPPLETIVE RELATIVE AL TRATTAMENTO PARTICOLARI DI DATI SENSIBILI

7.1. DESCRIZIONE GENERALE

CAPITOLO 8

PIANO DI VERIFICHE ED AGGIORNAMENTO DEL DPS

8.1 SCOPO

8.2. TEST DI VERIFICA DELL'ACCESSO FISICO AI LOCALI OVE SI SVOLGE IL TRATTAMENTO AUTOMATIZZATO

8.3 TEST DI VERIFICA DELLA SICUREZZA DELLE TRASMISSIONI IN RETE

8.4 TEST DI VERIFICA DELLE MODALITÀ DI REIMPIEGO DEI SUPPORTI DI MEMORIZZAZIONE

8.5 TEST DI VERIFICA DELLE PROCEDURE DI GESTIONE DELLE PAROLE CHIAVE E DEI PROFILI DI AUTORIZZAZIONE DEGLI INCARICATI

8.6 TEST DI VERIFICA DELLE PROCEDURE RELATIVE ALL'INTEGRITÀ E ALL'AGGIORNAMENTO DEI DATI PERSONALI

8.7 TEST DI VERIFICA DELLE MODALITÀ DI CONSERVAZIONE DEI DOCUMENTI

8.8 TEST DI VERIFICA DEL LIVELLO DI FORMAZIONE E DEL GRADO DI APPRENDIMENTO DEGLI INCARICATI

PARTE V
ELENCO ALLEGATI AL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Allegato 1 - n.15 fascicoli relativi ai singoli Settori, contenenti determinazioni dirigenziali misure minime e dettagli tecnici

Allegato 2 - Modulo nomina incaricati del trattamento

Allegato 3 - Linee guida e istruzioni operative agli incaricati per l'adozione di adeguate misure di sicurezza

Allegato 4 - Modello nomina incaricati esterni del trattamento

Allegato 5 - Modello nomina preposto custode parole chiave

Allegato 6 - Modello nomina amministratore di sistema

Allegato 7 - Modello nomina responsabili Esterni del trattamento

Allegato 8 - Accesso ai locali ed agli archivi

Allegato 9 - Report interventi formativi realizzati e da realizzare

Allegato 10 - Gestione dei rischi – Protezione aree e locali

Allegato 11 - Gestione dei rischi – Protezione ed integrità dei dati

Allegato 12 - Gestione dei rischi – Protezione trasmissione dati

Allegato 13 - Gestione dei rischi – Protezione strumenti non automatizzati

Allegato 14 - Report annuale rischi luoghi ove vengono trattati i dati

Allegato 15 - Report annuale virus

Allegato 16 - Report annuale rischi Hardware S.O. e applicazioni software

Allegato 17 - Registro salvataggio/ripristino banche dati

Allegato 18 - Registro distribuzione supporti di memorizzazione

Allegato 19 - decreto legislativo 196/2003 e disciplinare tecnico allegato

Allegato 20 - Regolamento Comunale sul trattamento dei dati sensibili e giudiziari

Allegato 21 - Informativa ai dipendenti

Allegato 22 - Vademecum esplicativo

INTRODUZIONE

Il presente documento programmatico sulla sicurezza dei dati personali è stato elaborato sulla base di quanto disposto del 19° comma del Disciplinare tecnico (artt.33 -36) del Nuovo Testo Unico in materia di trattamento di dati personali del 30.6.2003 n.196 e norme allo stesso collegate.
Tale documento, obbligatorio per chiunque tratti dati sensibili o esegua il trattamento di dati personali a mezzo di elaboratori elettronici, è stato elaborato a seguito di una dettagliata analisi dei rischi del trattamento potenzialmente presenti sia nei sistemi informativi che nei siti fisici del Comune di RAGUSA, tra questi compresi i luoghi individuare, analizzare ed applicare un complesso di contromisure di diverso genere per l'abbattimento dei rischi e per garantire la massima sicurezza in ordine al trattamento dei dati personali i cui aspetti e profili caratteristici sono anche riportati nel Vademecum Esplicativo del Trattamento dei dati personali che costituisce parte integrante ed indefettibile del presente documento.

Il Documento Programmatico sulla Sicurezza dovrà essere aggiornato dal Dirigente del Settore I con la collaborazione di tutti i Dirigenti di Settore, in quanto Responsabili del **Trattamento,** ogni anno (entro il 31 Marzo) e periodicamente modificato qualora nel corso del trattamento annuale dovessero insorgere anomalie applicative delle misure di sicurezza adottate o qualora dovessero ravvisarsi inadeguatezze anche in relazione a nuovi rischi.

Inoltre il Comune di RAGUSA farà menzione della redazione del presente documento nella relazione accompagnatoria al bilancio. Tale adempimento è obbligatorio e consiste nella dichiarazione che il documento programmatico è stato adottato o, per gli anni successivi, aggiornato. La mancanza di tale dichiarazione nella relazione accompagnatoria al bilancio configura un'ipotesi di vizio del bilancio per carenza di precisione e verità.

Inoltre il Comune di RAGUSA ha provveduto all'adozione di un regolamento comunale entro il 31/12/2005 e qualora la tipologia dei dati trattati e le operazioni eseguibili non siano state contemplate da una norma di legge provvederà ad aggiornarlo secondo le disposizioni di legge.

Il Comune di Ragusa in persona del Sindaco Titolare del Trattamento, è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione delle misure di sicurezza, sia idonee, sia minime. Il Titolare si avvale dei Responsabili del Trattamento individuati nei Dirigenti e nei singoli settori giusta Determinazioni Dirigenziali agli atti d'ufficio. per la predisposizione della modulistica, per la rilevazione dei rischi, e per la predisposizione e/o aggiornamento del Documento Programmatico sulla Sicurezza.

Di conseguenza, il Comune di RAGUSA, a seguito della rilevazione dei rischi cui è esposto, adotta le misure minime, ai sensi dell'allegato B " Disciplinare Tecnico" del D.Lgs. 196/2003, e procede alla predisposizione delle misure Idonee ritenute indispensabili nella struttura di riferimento.
Spetta ai titolari del trattamento, dopo aver valutato la congruità tecnico-economica delle misure proposte, disporre l'adozione delle stesse.
Le misure di sicurezza, individuate nell'ambito del presente documento, costituiscono un valido strumento non solo al fine della piena cognizione di quelle attualmente adottate e rilevanti ai fini della privacy ma anche, e soprattutto, per l'individuazione di quelle ancora necessarie per il pieno rispetto della riservatezza e di tutti gli altri principi che regolano la materia.

A tal fine il Consiglio Comunale ha adottato con deliberazione di Consiglio Comunale n. 62 del 30.12.2005 provvederà all'adozione del regolamento per il trattamento dei dati personali che, se necessario, verrà periodicamente aggiornato, mentre i Dirigenti provvederanno ciascuno per il proprio Settore all'adozione di tutti quei provvedimenti necessari all'adozione delle misure minime di sicurezza.

Sono responsabili del trattamento e costituiscono il Gruppo Privacy i Dirigenti dei Settori coordinati dal Dirigente del Settore Affari Generali, nonché eventuali responsabili esterni del trattamento. A seguito della suddetta nomina, il Comune di RAGUSA avendo predisposto la modulistica necessaria ai vari adempimenti sanciti dal D. Lgs 196/03, ha provveduto con singole Determinazioni dirigenziali a nominare i singoli incaricati del trattamento, conferendo loro le autorizzazioni necessarie avuto riguardo alle mansioni svolte da ciascuno, giusta quanto previsto dal Regolamento sul trattamento dei dati sensibili e giudiziari adottato con deliberazione di Consiglio comunale n. 62 del 30.12.2005.

Il presente documento è articolato in cinque parti ulteriormente divise in otto capitoli complessivi e diversi sottoparagrafi e da **diversi allegati con la sigla DPS/ALL.XX** nell'ultimo capitolo sono state riportate le modalità di controllo e di aggiornamento del documento che, in base a quanto previsto dal vigente Testo Unico in materia di trattamento di dati personali, deve essere sottoposto a revisione entro e non oltre ogni 31 marzo o comunque entro un anno dalla redazione del presente documento.

Riferimenti normativi
Art. 11 D.Lgs. 196/03
Modalità di raccolta e requisiti dei dati personali
Artt. 18-22 D.Lgs. 196/03
Regole ulteriori per i soggetti pubblici
Art. 31-36 D.Lgs. 196/03
Misure di Sicurezza dei dati
All. B
D.Lgs.196/03 e Disciplinare tecnico

CAPITOLO 1

INDIVIDUAZIONE E CLASSIFICAZIONE STRUTTURALE ED ORGANIZZATIVA DEL COMPLESSO DEI TRATTAMENTI DI DATI PERSONALI SENSIBILI E GIUDIZIARI

A seguito di una dettagliata analisi delle categorie di dati personali trattati nel Comune di Ragusa e delle relative banche dati effettuata congiuntamente dal Titolare e dai Responsabili del Trattamento, ulteriormente riportata nelle determinazioni allegate e nelle **schede di ciascun settore di cui in allegato**, è emerso che i dati personali oggetto di trattamento possono essere classificati sia all'interno della categoria dei dati comuni, sia in quella dei dati sensibili.
Effettuato questo preliminare e fondamentale esame, che ha avuto ad oggetto in particolare le banche dati trattate da ciascun Settore dell'Ente, al fine di individuare un corretto utilizzo dei dati medesimi, si è proceduto alla necessaria descrizione della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture e dei soggetti preposti al trattamento.
Considerato quanto sopra e ai sensi del punto 19.2 del Disciplinare tecnico D.Lgs.196/03 in ordine alla distribuzione dei compiti e delle responsabilità, si rimanda a quanto già specificato nel **Vademecum Esplicativo del Trattamento e agli allegati al DPS** che hanno permesso di predisporre la nomina e la distribuzione dei compiti ai singoli dipendenti-incaricati.
Pertanto, al fine di evitare inutili duplicazioni, si fa rinvio alle **determinazioni di nomina allegate al presente documento ("Modulo Nomina Incaricati del Trattamento")** al fine dell'individuazione dei soggetti nominati all'interno dell'ente comunale
All'interno dell'Ente possono essere detenuti sia dati comuni, sia dati sensibili e/o giudiziari.
In particolare per quanto riguarda i dati sensibili, la struttura può essere in possesso di :

1)dati idonei a rilevare le opinioni sindacali dei propri dipendenti;
2) dati idonei a rilevare lo stato di salute degli stessi;
3) dati idonei a rilevare l'origine razziale, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati , associazioni od organizzazioni a carattere religioso, filosofico, politico sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale dei cittadini.

Per quanto riguarda i dati giudiziali l'Ente può essere ni possesso di:

- dati riguardanti il casellario giudiziale
- dati riguardanti i carichi pendenti.

Il trattamento dei dati medesimi avviene con modi manuali e con l'ausilio anche di mezzi elettronici. I dati vengono assoggettati alle seguenti operazioni di trattamento:

- raccolta

- registrazione
- organizzazione
- conservazione
- elaborazione
- modificazione
- selezione
- estrazione
- raffronto
- utilizzo
- interconnessione
- comunicazione
- cancellazione
- distruzione

I dati di cui l'Ente è titolare sono trattati per le seguenti principali finalità:
- finalità istituzionali

nonché agli **allegati** riferiti a ciascun Settore, per la descrizione dell'intero procedimento di trattamento del dati.
Il trattamento dei dati effettuato dal Comune di Ragusa si svolge presso le seguenti sedi diverse distinte per Settori:

A) Settore I ,Corso Italia, 72, piano terra I, II piano e piano ammezzato lato destro, e varie sedi decentrate in Ragusa, Marina di Ragusa e San Giacomo;
B) Settore II, Piazza San Giovanni, II piano scala A;
C) Settore III, Corso Italia, 72 , II piano;
D) Settore IV, Via San Vito;
E) Settore V, Corso Italia, piano terra e piano ammezzato lato sinistro;
F) Settore VI, Piazza San Giovanni, II piano scala A;
G) Settore VII, Piazza San Giovanni, I,II,III,IV piano, scala B;
H) Settore VIII, Piazza Pola, I e II piano;
I) Settore IX, Piazza San Giovanni e varie sedi decentrate a Ragusa e Marina di Ragusa, magazzini Via M Spadola
J) Settore X, Via M. Spadola, e sedi decentrate;
K) Settore XI, Piazza San Giovanni, scala A;
L) Settore XII, Piazza San Giovanni e sedi decentrate;
M) Settore XIII, Piazza San Giovanni e sedi decentrate;
N) Settore XIV, Via M.Spadola e sedi decentrate
O) Settore XV, corso Italia,72.

Gli archivi cartacei, gli elaboratori, i supporti informatici si trovano tutti all'interno dei detti siti. In particolare, i dati acquisiti su supporti cartacei si trovano custoditi nei locali indicati con le modalità individuate dai singoli responsabili con separato atto.

I locali dove sono custoditi i dati non sono accessibili al pubblico. L'accesso, è comunque sempre controllato ed inibito agli estranei.

CAPITOLO 2

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI PERSONALI IN RELAZIONE AI SISTEMI DI ELABORAZIONE DEI DATI

L'analisi del rischio del trattamento dei dati personali è ritenuto un adempimento di fondamentale importanza sia per riflettere sui tratti cd. deboli del sistema di protezione sia ed a maggior ragione per individuare nel dettaglio le più efficienti misure minime di sicurezza a protezione dei dati personali trattati.
Pertanto ciascun incaricato dovrà creare una parola chiave secondo le direttive del disciplinare tecnico ed illustrata nel Vademecum Esplicativo del Trattamento, scriverla e consegnarla in busta chiusa al custode (Dirigente di Settore o suo delegato) delle parole chiave.
In tal modo, in caso di assenza dell'incaricato, qualora si rendesse necessario accedere alle banche dati di sua esclusiva competenza, sarà sufficiente aprire la busta consegnata al custode e procedere alle operazioni necessarie.
Dall'analisi effettuata presso il Comune di Ragusa è emerso inoltre che i rischi connessi al trattamento dei dati personali possono suddividersi in base a due grandi categorie ed in particolare:
RISCHI CONNESSI AL MANCATO RISPETTO DEGLI ADEMPIMENTI E DELLE PRESCRIZIONI STATUITE DAL NUOVO TESTO UNICO IN MATERIA DI TRATTAMENTO DI DATI PERSONALI;
RISCHI PROPRI DEL SISTEMA INFORMATIVO UTILIZZATO NELL'ENTE.
Tale distinzione si chiarisce se si considera che i rischi del trattamento della prima categoria si riferiscono direttamente ed unicamente all'intera materia inerente la tutela dei dati personali mentre i rischi sottesi alla seconda si riferiscono all'applicazione pratica, effettiva e funzionale delle misure di sicurezza adottate, tra queste comprese quelle relative alla sicurezza informatica.
L'analisi del rischio è stata, pertanto, affrontata secondo quanto sopra riportato e di conseguenza suddivisa in due settori di rischi propri nettamente differenti e separati per tipologia e materia.
PRIMO SETTORE DI RISCHIO:
In questa fase dell'analisi sono stati individuati e valutati tutti i rischi previsti dalla legge, quali, ad es. il rischio di distruzione accidentale dei dati, il rischio di perdita dei dati, il rischio di accesso non autorizzato, il rischio di trattamento di dati non conforme alla finalità della raccolta, il rischio di trattamento illegittimo e di trattamento non consentito, ecc..
A tal proposito si è ritenuto fondamentale arginare il menzionato problema innanzitutto con un adeguato ed efficiente piano di formazione degli incaricati del trattamento (v. successivo cap.5) e ciò in quanto è dato riscontrare che la maggior parte delle violazioni della privacy vengono perpetrate direttamente e quasi unicamente dagli incaricati del trattamento.

Infatti proprio tali soggetti sono potenzialmente idonei ad effettuare in astratto comunicazioni o diffusioni illegittime di dati personali o di utilizzare tali dati per fini non conformi alle finalità del trattamento.
Di tale settore di rischio è necessario occuparsi quindi mediante l'approfondita conoscenza della legge sulla Privacy.
Si è ritenuto, infatti, che solo un'adeguata conoscenza del disposto normativo possa realmente e proficuamente garantirne l'osservanza del medesimo ed in definitiva possa abbattere effettivamente i rischi connessi a tale primo settore.

SECONDO SETTORE DI RISCHIO:
In questa fase, invece, sono stati identificati e valutati i rischi del sistema informativo e tutti quelli che sono propri della sua normale attività.
Al fine di verificare quali misure siano necessarie, il Dirigenti di Settore Responsabili del Trattamento, provvedono ad adottare una serie di azioni, che si concretizzano in una
dettagliata individuazione e valutazione dei rischi connessi al Trattamento dei dati personali.
Si è ritenuto, pertanto, procedere all'individuazione dei beni e dei dati da tutelare, al fine dell'adozione delle misure minime di sicurezza.
Le risorse da tutelare possono essere distinte in:
HARDWARE;
SOFTWARE;
DATI (COMUNE E/O SENSIBILI);
DOCUMENTAZIONE CARTACEA;
SUPPORTI DI MEMORIZZAZIONE.
Verificati i dati raccolti, in sede di monitoraggio del processo di trattamento e ricostruito il flusso delle informazioni si è ritenuto essenziale procedere all'analisi dei rischi, che si concretizza nell'individuazione dei fattori di rischio e nella loro successiva valutazione.
Le fasi che caratterizzano questo processo sono tre:
analisi: attraverso l'uso di apposite check-list sono stati monitorati i rischi per le informazioni trattate, ma anche quelli relativi alle aree e ai locali e alle modalità di Trattamento, in particolare ai collegamenti in rete (DPS/ALL 10 – 11 – 12 – 13);
valutazione: una volta evidenziati i rischi, presenti in ogni unità complessa di Trattamento oppure di base di Trattamento, si è provveduto ad assegnare ad ogni
fattore di rischio un indice numerico relativo alla frequenza e all'incidenza del rischio stesso;
trattamento: dopo aver ottenuto il fattore rischio, che è dato dal prodotto dell'indice della probabilità del verificarsi dell'evento per quello della gravità del danno, si deve procedere all'adozione delle misure specifiche di sicurezza per ogni fattore. È ovvio che occorre adottare tali misure a seconda della tipologia di strumenti utilizzati e della natura dei dati trattati.

2.1 CRITERI PER LA VALUTAZIONE DEI RISCHI

Individuati i rischi si è proceduto alla valutazione degli stessi, attraverso una indicizzazione delle possibili perdite. In particolare si è tenuto conto di due indici:
probabilità (P) di accadimento, che riguarda la frequenza riscontrata o riscontrabile;
magnitudo (M) delle conseguenze, nel caso lo stesso evento si verifichi.
Il Rischio è la risultante della probabilità e della gravità di un evento: l'indice R è quindi dato dal prodotto P X M.
Secondo i criteri adottati dando a P un valore tra 1 e 4 e a M ugualmente tra 1 e 4, si è ottenuto il valore R compreso fra 1 e 16.

Probabilità (P)

1: Improbabile Non sono noti episodi.
2: Poco probabile Sono noti rarissimi episodi.
3: Probabile Noto qualche episodio in cui la mancanza rilevata ha fatto seguito a un danno.
4: Altamente probabile Si sono verificati danni per la stessa mancanza rilevata in situazioni simili.

Magnitudo (M)

1: Lieve Distruzione dei dati
2: Medio Utilizzo illegale o alterazione dei dati
3: Grave Perdita di dati causata da un uso non autorizzato da parte di un incaricato.
4: Gravissimo Furto o Perdita dei dati a seguito di diffusione illegale.

Da ciò consegue che proprio nella fase di valutazione dei rischi si dovranno verificare:
l'efficacia degli strumenti adottati, e ciò al fine di assegnare al rischio un indice di gravità (quali danni sono stati riscontrati o quali ancora possibili) e di frequenza (intesa a verificare, nonostante la misura adottata) e quindi di individuare le circostanze di manifestazione di attacchi informatici al fine di individuarne anche le consequenziali azioni correttive; le misure che sono risultate non adeguate.
Il processo di individuazione ed ulteriore valutazione dei rischi eventualmente manifestatisi sarà ripetuto con cadenza almeno annuale e, comunque, immediatamente al verificarsi di rischi gravi connessi al trattamento.

2.2 MISURE DI PREVENZIONE E PROTEZIONE

Le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:
la prevenzione: attività che permette di impedire gli accadimenti negativi, agendo direttamente sulla diminuzione delle probabilità di manifestazione dei rischi;
la protezione: attività che permette di diminuire la gravità degli effetti causati eventualmente dall'accadimento dell'evento rischio.
Dopo aver analizzato e valutato i fattori dei rischi relativi alle aree, ai locali, all'integrità dei dati e alle trasmissioni, sono state individuate le misure di prevenzione e protezione più idonee per ridurre ed eliminare il rischio stesso.
L'insieme delle misure preventive e protettive costituisce un programma dinamico di fondamentale importanza nell'ambito della politica per la Sicurezza dei dati informatici.
Tale previsione assolve alla funzione di guida operativa a supporto della gestione della Sicurezza del trattamento dei dati personali.
L'onere di provvedere al tempestivo intervento è stato riassunto con un cd. scadenzario degli interventi contrassegnato al suo interno con un parametro di "n" mesi crescenti in funzione inversa all'indice di gravità (e quindi al valore del numero arbitrario "R").
Vedere esempio seguente:
R = 16 intervento entro 01 mesi e verifica entro 10 giorni
R = 12 intervento entro 04 mesi e verifica entro 20 giorni
R = 08 intervento entro 08 mesi e verifica entro 30 giorni
R = 04 intervento entro 12 mesi e verifica entro 40 giorni
R = 01 intervento entro 16 mesi e verifica entro 60 giorni.

Misure Organizzative
01 Analisi dei rischi
02 Redazione linee-guida sicurezza
03 Istruzioni interne e formazione professionale degli incaricati
04 Assegnazione incarichi
05 Elaborazione dati
06 Classificazione dei dati
07 Misure graduate per classi dati
08 Consultazioni registrate
09 Controlli periodici
10 Verifiche periodiche per finalità
11 Sorveglianza sulla distruzione sup.
12 Altro

Misure Fisiche
01 Vigilanza della sede
02 Ingresso controllato

03 Sistemi di allarme
04 Registrazione accessi
05 Autenticazione accessi
06 Custodia in classificatori o armadi
08 Custodia in armadi blindati
09 Dispositivi antincendio
10 Continuità elettrica
11 Verifica leggibilità supporti
12 Altro

Misure Logiche
01 Identificazione utente
02 Autenticazione utente z.
03 Controllo accessi
04 Registrazione accessi
05 Controlli antivirus
06 Sottoscrizione elettronica
07 Cifratura dati trasmessi 08 Cifratura dati memorizzati
09 Annotazione fonti dei dati
10 Annotazione responsabile opera
11 Rilevazione intercettazioni
12 Monitoraggio continuo sessioni
13 Sospensione automatica sessioni
14 Verifiche automatizzate dati
15 Controllo supporto dati manutenzione
16 Altro

CAPITOLO 3

INDIVIDUAZIONE DELLE MISURE DI CONTROLLO DEI RISCHI PER GARANTIRE L'OSSERVANZA DELLE NORME SULLA PRIVACY

3.1 PROCEDURE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI IN RIFERIMENTO ALLE MISURE DI SICUREZZA FISICHE, ELETTRONICHE E PROCEDURALI DI TUTTI I SITI DEL TRATTAMENTO DEI DATI.

3.2. ELENCAZIONE DELLE MISURE DI PROTEZIONE DELLE AREE E DEI LOCALI IN RIFERIMENTO AL CONTROLLO FISICO E LOGICO DEGLI ACCESSI.

Premesso che l'obiettivo auspicabile è quello dell'eliminazione integrale ed assoluta dei rischi deve rilevarsi che esso non è raggiungibile in forma sistematica a causa della pur sempre presente potenzialità di verificazione dello stesso.
Sovente, infatti, la natura dei luoghi rende difficoltosa l'adozione di efficienti misure di protezione in quanto è impossibile affermare che l'evento dannoso non possa verificarsi in assoluto.
Quello che logicamente ed obiettivamente è concretamente realizzabile è la cd. prevenzione perché consente di diminuire le probabilità di manifestazione dei danni.
Tale aspetto si fonda sulla individuazione preliminare e successiva applicazione di varie contromisure potenzialmente idonee ad ostacolare l'intrusione e/o l'utilizzazione illegittima dei dati personali.
Effettuata una dettagliata analisi del trattamento dei dati sono state individuate una serie di misure di protezione particolarmente efficaci in quanto volte a garantire e proteggere contemporaneamente diverse aree di rischio.
Questo tipo di misure di prevenzione è stata classificata in tre categorie:
Misure di difesa fisica.
Misure di difesa elettronica.
Misure di difesa di tipo procedurale.

Le misure di SICUREZZA FISICA sono quelle che impediscono e/o rallentano eventuali intrusioni da parte di soggetti non autorizzati.
Considerato che i potenziali rischi connessi al trattamento sono anche rischi che riguardano ed involgono le aree ed i locali tali misure si rendono pertanto necessarie ed indefettibili.
A tal proposito è da dire che le misure adottate dal Comune di Ragusa sono pressoché uguali in tutti i siti nei quali si svolge l'attività comunale sono:
Dispositivi antincendio (estintori)
Rilevatori fumo (nelle sedi dotate)
Selezione degli accessi mediante personale posto all'ingresso della sede

Custodia dei dati in armadi e classificatori chiusi a chiave.
In relazione a tale ultima misura di sicurezza, v'è da precisare che non tutti gli armadi e i classificatori che contengono dati personali possono essere chiusi a chiave in quanto non dotati di idonea serratura. Al fine di soddisfare gli adempimenti previsti dalla legge il Comune di Ragusa valuterà la spesa necessaria all'acquisto degli armadi o classificatori adeguati oppure, in alternativa, ad adeguare gli armadi già in uso, ove possibile, alle prescrizioni di legge mediante l'acquisto di lucchetti.
Tali misure, possono essere in linea di principio, ritenute idonee ad assicurare un minimo di protezione dei locali, tenuto conto del mancato verificarsi di eventi quali l'intrusione di soggetti esterni non autorizzati o l'incendio dei locali ove si trovano i dati personali.
Lo stesso non può dirsi per i locali destinati ad archivio. Allo stato attuale gli archivi storici non godono di adeguata protezione dai rischi di natura fisica in quanto sono allocati in stanze all'uopo predisposte presso le diverse sedi comunali ma non protette da misure idonee alla riduzione dei rischi di natura fisica. Allo stato attuale solo la chiusura della porta d'ingresso alla stanza costituisce la protezione contro gli accessi abusivi.
L'adozione di procedure per la gestione delle chiavi e la registrazione degli accessi all'archivio è ritenuta misura idonea che completerebbe le misure di tutela richieste contro gli accessi abusivi.

Le misure di DIFESA ELETTRONICA che sono state previste ed installate nella sede principale e in quelle secondarie consistono in:
Piano di emergenza (nelle sedi ove previsto)
Certificato impianto elettrico
Copie di back-up delle banche dati vengono effettuate periodicamente, ogni sette giorni oppure in un termine diverso se ve ne è necessità.
Il collegamento a Internet è effettuato tramite ADSL è protetto in quasi tutte le postazioni da programmi antivirus o da sistemi analoghi.
La trasmissione di dati in formato elettronico, viene effettuata tramite e-mail di cui viene sempre verificato il buon fine e di cui viene effettuata una copia di salvataggio.
La posta elettronica viene gestita a mezzo di un apposito software.
I fax sono allocati presso le stanze degli incaricati. Alcune macchine sono condivise fra incaricati dello stesso servizio, altre invece sono riservate ad un unico utente.
Quasi tutti I PC sono dotati di password. **Si rinvia alle schede per ciascun settore allegate al presente** documento per una migliore analisi di dettaglio.
Le misure di sicurezza di tipo elettronico adottate dal Comune di Ragusa, valutate in relazione al rischio, sono ritenute sufficienti alla tutela dei dati trattati.
In relazione alle banche dati trattate dai vari Settori, nei casi in cui i p.c. sono collegati tramite rete, è necessario predisporre la rete informatica in maniera da consentire a ciascun incaricato solo l'accesso alle banche dati necessarie allo svolgimento della propria mansione.

Le misure di TIPO PROCEDURALE consistono nella gestione e nella manutenzione accurata degli impianti e strumenti elettronici, nella effettuazione di ispezioni a al fine di verificare l'applicazione e l'osservanza delle istruzioni impartite agli incaricati, l'effettuazione delle copie di back-up, la verifica costante del regolare ed efficiente funzionamento delle serrature degli armadi e della compartimentazione dei locali, ecc.
Sempre nell'ordine di tale tipo di misure sono stati assegnati specifici incarichi ai collaboratori interni ed individuati come incaricati del trattamento dei dati personali.
A tali soggetti sono state assegnate delle credenziali di autenticazione, password e codici identificativi, strettamente personali e regolarmente formati in ossequio alle norme in materia di Privacy secondo quanto specificato in appresso.
Inoltre, periodicamente si provvederà alla verifica della rispondenza dei profili di autorizzazione degli incaricati del trattamento e alla loro modifica, se necessario. Tale adempimento verrà effettuato almeno una volta ogni anno e se non saranno state necessarie modifiche si provvederà a riportare i profili di autorizzazione attuali nel Documento Programmatico sulla Sicurezza per l'anno 2008.
Quanto alla trasmissione dei dati, oltre alla procedura per la gestione della posta elettronica sopra illustrata, il Comune di Ragusa trasmette dati all'esterno sia attraverso il fax, sia brevi manu, sia a mezzo corriere con tutte le cautele richieste dal caso.
Il Comune di Ragusa provvederà al costante monitoraggio anche dei dati trattati soprattutto al fine del controllo e della comparazione con quelli il cui trattamento è autorizzato in quanto dati definiti di rilevante interesse pubblico.

CAPITOLO 4

DESCRIZIONE DEI CRITERI E DELLE MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI PERSONALI

Il presente capitolo è stato elaborato in riferimento al punto 19.5 del disciplinare tecnico del D.Lgs. 196/2003 che impone "la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23. Il successivo punto 23 richiamato stabilisce inoltre che "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".
Inoltre, con riferimento al punto 18 stabilisce che "sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale".
Considerato che ogni sistema informatico deve prevedere un piano di emergenza per soddisfare le specifiche del disciplinare tecnico è necessario, pertanto, riferirsi alle modalità operative già applicate dall'Ente e come tali raffigurate in semplici procedure o istruzioni operative per il salvataggio dei dati e per il ripristino in caso di distruzione, perdita o inaccessibilità dei dati, le modalità per ricostruirli e ripristinare il servizio.
È il Dirigente di ciascun settore che provvederà ad impartire i singoli dipendenti o comunque chi è responsabile del salvataggio e ripristino dei dati dei singoli uffici amministrativi, utilizzando apposite schede di cui in allegato al presente documento programmatico sulla sicurezza.
Quanto affermato muove dalla considerazione che ogni giorno nuovi virus si propagano rapidamente e che gli stessi sono causa di notevoli danni che a volte raggiungono proporzioni gigantesche.
I Dirigenti di Settore nel prestare molta attenzione a questo aspetto hanno ritenuto opportuno, oltre che installare ed aggiornare periodicamente gli antivirus, prevedere una serie di procedure di recupero immediato dei dati in caso di attacchi e, comunque, delle copie di salvataggio dei dati personali trattati.
Qualora l'evento dannoso sia di facile soluzione, il Comune attiverà la procedura per il ripristino dei dati mediante le copie dei dati effettuate da ciascun incaricato su floppy disk o su CD rom. In caso contrario si provvederà a delegare una ditta esterna specializzata nel settore informatico.

CAPITOLO 5

DISAMINA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO

5.1 SCOPO DELLA FORMAZIONE

La previsione degli interventi formativi degli incaricati del trattamento rientra tra gli aspetti più importanti del presente documento programmatico sulla sicurezza. Infatti, si è ritenuto che possa parlarsi di effettiva sicurezza del trattamento solo in costanza di un idoneo piano di formazione degli incaricati. Tale formazione è stata ritenuta alla stessa stregua di un elemento fondamentale per il raggiungimento degli obiettivi prefissati ed in particolare per quello della sicurezza del trattamento dei dati personali.

E' stato ritenuto, inoltre, che la predisposizione e l'applicazione di sofisticati strumenti di sicurezza, informatica e non, non garantiscano la stessa in modo assoluto senza le capacità e/o le adeguate conoscenze del personale chiamato alla loro gestione. Una gestione impropria da parte degli operatori, la mancanza di chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione costituiscono le cause principali per la verificazione anche inconsapevole di danni agli interessati ed in definitiva la causa prioritaria dell'inadeguatezza.

Quanto premesso trova effettivo riscontro nel comma 19.6. del D.Lgs. 196/2003 che impone, infatti, "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."

5.2 TECNICHE E STRUMENTI DI FORMAZIONE DEGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI.

Tra gli aspetti salienti della disamina degli interventi formativi degli incaricati del trattamento il Comune di Ragusa ha ritenuto necessario ed indispensabile prevedere un adeguato e dettagliato piano di formazione.

Tra le varie tecniche didattiche si ritiene più proficua quella della lezione tenuta direttamente da un esperto nella consulenza e nell'assistenza dello specifico settore in materia di trattamento dei dati personali. Al fine della maggiore incisività della tecnica didattica prescelta si è ritenuto, inoltre, che il corso formativo sia presentato con slide esplicative. Oltre tali adempimenti, gli incaricati presenti al corso di

formazione sono corredati da materiale cartaceo esplicativo della legge, degli adempimenti richiesti dalla medesima nonché delle misure minime di sicurezza. Infine si prevedono anche attività periodiche di aggiornamento in relazione ad interventi legislativi, pareri del Garante della Privacy, giurisprudenza e nuova dottrina nelle varie casistiche, che sono inviate a ciascun Dirigente.

5.3. CONTENUTO DEL PIANO DI FORMAZIONE

Considerata l'importanza e la necessità della formazione degli incaricati del trattamento dei dati personali si è ritenuto indispensabile analizzare nel dettaglio il contenuto del piano di formazione che, pertanto, è stato così suddiviso e deve contenere i seguenti passaggi logico-giuridici:

-Introduzione al D. Lgs 196/03 e cenni storici
-Principali definizioni
-Principi fondamentali (artt. 1, 2, 7, 11)
-I rischi, la loro prevenzione e il loro abbattimento -
- Principi relativi al trattamento effettuato dagli enti pubblici
- Istruzioni operative relative ai principali trattamenti svolti in ambito comunale
- Il soggetto interessato. I suoi diritti e loro tutela
- I soggetti degli artt. 28-30 D. Lgs 196/03. Qualità e responsabilità. Istruzioni operative
- L'informativa
- Obblighi di sicurezza
- Misure di sicurezza per trattamenti informatizzati e non
- Misure di sicurezza fisiche
- Il Documento programmatico sulla sicurezza
- Responsabilità civile verso l'interessato
- Responsabilità amministrativa e penale e relative sanzioni
- Il Garante per la Privacy
- Dibattito

Tali aspetti concretizzano la diretta ed effettiva formazione degli incaricati del trattamento dei dati personali per la specifica considerazione che i Responsabili del Trattamento dei dati personali non possono essere sempre presenti in ogni fase del trattamento che, viceversa, prevede la delega all'incaricato dell'applicazione quotidiana delle misure minime di sicurezza.
Si è ritenuto, pertanto, che solo se l'incaricato si rende esattamente conto del suo ruolo, della delicatezza e dell'importanza dei dati personali a lui affidati, l'Ente potrà realmente garantirsi contro il rischio di trattamenti di dati personali non conformi alle finalità della raccolta e/o contro il rischio di trattamenti illeciti.

5.4. VALUTAZIONE DELL'EFFICIENZA DEL PIANO DI FORMAZIONE

Il Dirigente, dopo avere dettagliatamente individuato il contenuto del piano di formazione, grazie anche al sostegno di consulenti esperti in materia, possono ritenere importante approntare una serie di strumenti di verifica dell'efficienza della formazione e ciò in quanto è necessario essere certi che la formazione impartita sia stata realmente recepita dagli incaricati del trattamento e che sia stata, soprattutto, utile ad un appropriato e sicuro trattamento dei dati personali.

Per quanto detto, a seguito dei percorsi formativi sul trattamento dei dati personali, potrà essere utilizzato un questionario da sottoporre ai partecipanti a fine corso per effettuare una dettagliata valutazione dell'efficacia del loro apprendimento. Pertanto, sarà utile utilizzare degli indici che debbono essere legati ai principali obiettivi della valutazione ed in particolare:

offrire informazioni che permettano all'incaricato di auto-valutare in futuro la propria prestazione nel campo del trattamento dei dati personali;

offrire informazioni di supporto al supervisore nella valutazione dell'incaricato;

contenere indicazioni per il responsabile della formazione e per il docente al fine di migliorarne le tecniche di insegnamento e di apprendimento;

5.5 AGGIORNAMENTO FORMATIVO E PROGRAMMI INDIVIDUALI DI FORMAZIONE ED ADEGUAMENTO

Dopo avere affrontato nel dettaglio l'importanza di tale adempimento deve, comunque, ricordarsi che la formazione deve essere sempre aggiornata in base al disposto del D.Lgs n.196/2003 in coincidenza con l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza.

In particolare deve effettuarsi e tenersi ben presente una chiara distinzione tra:

AGGIORNAMENTO PERIODICO.

L'aggiornamento periodico sarà adempiuto sotto la diretta vigilanza dei Dirigenti i quali vi provvederanno di concerto con il Dirigente del Settore I con cadenza almeno annuale.

AGGIORNAMENTO SPECIFICO.

L'aggiornamento specifico sarà tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e diverse procedure. Infatti, se l'incaricato viene assegnato a nuove mansioni o se viene trasferito da un settore ad un altro deve essere effettuato un nuovo aggiornamento mediante un programma individuale che deve essere organizzato e gestito dal Dirigente del settore cui appartiene l'incaricato con il diretto coinvolgimento dell'ufficio personale.

Quanto sopra riportato impone l'attivazione di aggiornamento in relazione alla specifica attività di trattamento svolta.

5.6 ATTIVITÀ DI FORMAZIONE

Nell'anno appena trascorso è stata avviata la formazione per tutti i Dirigenti e gli incaricati del Trattamento secondo le linee di indirizzo dei precedenti paragrafi.

CAPITOLO 6

DESCRIZIONE DELLE MISURE E DEI CRITERI DI INTERVENTO IN CASO DI TRATTAMENTI DI DATI PERSONALI AFFIDATI A STRUTTURE ESTERNE (OUTSOURCING)

6.1 SCOPO E LISTA DI CONTROLLO DELLE STRUTTURE ESTERNE

Il presente capitolo del Documento Programmatico sulla Sicurezza muove dalla considerazione che non sempre i Titolari del Trattamento possono gestire direttamente o per il tramite della struttura o servizio amministrativo dell'Ente di appartenenza i dati personali oggetto del trattamento.

Ci sono casi e situazioni per le quali il trattamento deve essere effettuato per il tramite di strutture esterne operanti in nome e per conto del Titolare; si pensi alla tesoreria comunale, a cooperative o società per l'assistenza domiciliare, ecc.

Questi soggetti agiscono per finalità definite dall'Ente e quindi non hanno poteri decisionali autonomi. Tale circostanza rende opportuno procedere alla loro nomina come Responsabili in out-sourcing utilizzando l'apposito modulo in allegato (DPS/ALL 11) previa l'esibizione da parte di tali soggetti dell'intera documentazione comprovante l'osservanza dei precetti imposti dalla Legge sulla Privacy.

La nomina può essere effettuata sia nei confronti di un soggetto fisico che nei confronti di un soggetto giuridico i quali, a seconda dei casi, saranno designati come contitolari del trattamento, se ne assumono la completa responsabilità, oppure responsabili esterni se i dati sono assunti o trattati sotto la diretta vigilanza e responsabilità del titolare primario.

Considerato che nella maggior parte dei casi la struttura esterna opera sotto la veste di responsabile del trattamento dei dati personali si ritiene che l'obbligo di vigilanza previsto dal codice permane totalmente a carico del Comune di Ragusa, Titolare del Trattamento.

Considerato però che dall'esperienza già maturata e dagli interventi dell'autorità Garante è emerso che il discarico di responsabilità non può considerasi realmente rispondente alla concreta situazione fattuale, è stato ritenuto, quindi, maggiormente rispondente al nuovo dettato legislativo che debba prevedersi una sorta di responsabilità congiunta fra il Titolare del Trattamento ed il Responsabile in Out-sourcing poiché quest'ultimo deve fornire una prova certa di essere in grado e di potere legalmente effettuare i trattamenti assegnati in condizioni tali da rispettare almeno le misure minime di sicurezza.

Premesso quanto sopra, al fine del corretto rapporto tra struttura esterna ed interna, è necessario sottoscrivere un idoneo contratto al fine di regolarne il rapporto in maniera effettivamente garantista per l'Ente ed in definitiva per gli interessati cui i dati si riferiscono. Tale Contratto prevede l'obbligo a carico del responsabile del Trattamento in out-sourcing di salvaguardare la riservatezza dei dati personali affidati, di utilizzare per il trattamento dei dati solo soggetti di comprovata fiducia e di essere in regola con le prescrizioni del testo Unico in materia di trattamento di dati

personali previa esibizione di idonea documentazione descrittiva dell'organizzazione esterna per meglio comprendere come le responsabilità sulla sicurezza sono distribuite in strutture che talvolta sono variamente articolate.
La nomina dei responsabili esterni spetta al Titolare (ossia ai Dirigenti di Settore), che dovrà prevederla negli atti di conferimento di incarichi (convenzioni, protocolli), o comunque dovrà essere prevista, per poi essere formalizzata con successivo atto Dirigenziale nei contratti stipulati dall'Ente.
A tali Responsabili esterni deve essere consegnata la lettera con la specificazione analitica dei compiti assegnati e delle istruzioni relative **(DPS/ALL 11)**, costituenti parte integrante dell'atto di conferimento ed avente natura amministrativa (concessione) o privata (contratto, convenzione).
Periodicamente i Dirigenti devono procedere al controllo sulle attività svolte dai Responsabili esterni, anche mediante verifiche periodiche sul campo.
Nominare un soggetto esterno Responsabile del Trattamento ha inoltre un altro vantaggio rilevante: comporta che il trasferimento di dati personali dall'Ente al soggetto esterno non sia qualificabile tecnicamente come una comunicazione di informazioni, con tutto ciò che questo comporta. Infatti le comunicazioni di dati personali da un soggetto pubblico nei confronti di un privato possono avvenire solo se ciò sia espressamente previsto da una legge o da un regolamento, secondo quanto previsto dall'art. 19 comma 3 del D.Lgs. 196/03. Nominare il soggetto privato
come Responsabile del Trattamento fa sì che venga meno il cd. rapporto di terzietà di quest'ultimo rispetto al legame Titolare - interessato al Trattamento: quindi la conoscenza dei dati di quest'ultimo, da parte del soggetto esterno, non sarebbe configurabile tecnicamente come una comunicazione. Quest'ultima infatti è definita come "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".
A completamento di quanto sopra specificato, i soggetti nominati come responsabile esterni dovranno essere inseriti in un elenco che dovrà essere reso conoscibile a chiunque, tramite affissione all'albo pretorio Comunale o tramite richiesta all'U.R.P. o tramite richiesta anche telefonica ai Responsabili dei vari Servizi.
A tal fine il Comune di Ragusa si avvale **dell'elenco agli atti di ciascun settore**.

CAPITOLO 7

MISURE DI SICUREZZA SUPPLETIVE RELATIVE AL TRATTAMENTO DI PARTICOLARI DATI SENSIBILI.

7.1. DESCRIZIONE GENERALE

Il presente capitolo evidenzia le ulteriori misure in caso di trattamento di dati sensibili o giudiziari richieste dal disciplinare tecnico del D.Lgs. n. 196/2003 ed in particolare dal punto 20 del disciplinare tecnico secondo quale" 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" ed il successivo punto 21 che stabilisce, inoltre, che "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", oltre ancora il punto 22 secondo il quale "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".

Per quanto riportato nel detto disciplinare il punto 23 prescrive che "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.

Per quanto sopra riportato non v'è dubbio che la protezione crittografica dei dati cui si riferisce lo stesso Testo Unico in materia di trattamento di dati personali rappresenti un prezioso strumento di tutela e di sicurezza contro i rischi di accesso ai dati personali.

CAPITOLO 8

PIANO DI VERIFICHE ED AGGIORNAMENTO DEL DPS

8.1 SCOPO

A completamento degli adempimenti e delle misure evidenziate nel presente Documento programmatico sulla Sicurezza dei dati personali i Titolari hanno ritenuto necessario ed opportuno predisporre un piano di verifica delle singole misure adottate. Tale previsione muove dalla considerazione che non esiste piano di sicurezza che possa garantire la sua efficacia se esso non viene verificato periodicamente. Prima di individuare nel dettaglio le singole procedure di verifica si riportano riassuntivamente le singole aree di rischio e ciò al fine di una reale e più completa verifica dell'efficienza del sistema individuato.
Specificamente le aree di rischio sono:
Accesso fisico ai locali ove si svolge il trattamento automatizzato;
La sicurezza delle trasmissioni in rete;
Le modalità di reimpiego dei supporti di memorizzazione;
Le procedure di gestione delle parole chiave e dei profili di autorizzazione degli incaricati;
Le procedure di verifica dell'integrità e dell'aggiornamento dei dati personali;
Le modalità di conservazione dei documenti.
Il livello di formazione ed il grado di apprendimento degli incaricati.
Per quanto sopra evidenziato si passano in rassegna i singoli test di seguito suddivisi in base al seguente ordine.
8.2. Test di verifica dell'accesso fisico ai locali ove si svolge il trattamento automatizzato;
8.3 Test di verifica della sicurezza delle trasmissioni in rete;
8.4 Test di verifica delle modalità di reimpiego dei supporti di memorizzazione;
8.5 Test di verifica delle procedure di gestione delle parole chiave e dei profili di autorizzazione
degli incaricati;
8.6 Test di verifica delle procedure relative all'integrità e all'aggiornamento dei dati personali;
8.7 Test di verifica delle modalità di conservazione dei documenti.
8.8 Test di verifica del livello di formazione e del grado di apprendimento degli incaricati.

8.2. TEST DI VERIFICA DELL'ACCESSO FISICO AI LOCALI OVE SI SVOLGE IL TRATTAMENTO AUTOMATIZZATO

Tale adempimento muove dalla considerazione che i luoghi ove si svolge il trattamento debbono essere necessariamente protetti contro il rischio di intrusioni fisiche. Per quanto detto saranno verificate periodicamente la solidità e l'efficienza

delle chiusure e le serrature esterne dei locali ed in particolare delle porte di accesso esterno e delle finestre nonché dei vetri delle medesime.
Inoltre sarà verificata periodicamente l'efficienza dei sistemi di antincendio di cui l'Ente è dotato con precipua attenzione all'efficienza degli estintori nonché allo stato di conoscenza e di aggiornamento del loro utilizzo da parte dei dipendenti e di quanti operano nella struttura. L'effettuazione di tale test e dei risultati ad esso sottesi sarà menzionata ed inserita nell'aggiornamento del successivo Documento Programmatico sulla Sicurezza ed i punti critici eventualmente riscontrati posti alla base delle necessarie ed indefettibili modifiche che dovranno essere apportate al nuovo piano di sicurezza del trattamento dei dati personali.

8.3 TEST DI VERIFICA DELLA SICUREZZA DELLE TRASMISSIONI IN RETE

Con questo adempimento saranno verificate le linee telefoniche, la presenza di eventuali usure e/o manomissioni delle stesse nonché l'efficienza della funzionalità degli apparati. Infine, a completamento di tale test, saranno essere verificate le procedure di identificazione del mittente nonché della verifica del destinatario.
L'effettuazione di tale test e dei risultati ad esso sottesi deve essere menzionata ed inserita nell'aggiornamento del successivo Documento Programmatico sulla Sicurezza ed i punti critici eventualmente riscontrati posti alla base delle necessarie ed indefettibili modifiche che dovranno essere apportate al nuovo piano di sicurezza del trattamento dei dati personali.

8.4 TEST DI VERIFICA DELLE MODALITÀ DI REIMPIEGO DEI SUPPORTI DI MEMORIZZAZIONE

Questo specifico test mira ad evitare e verificare che tutti i supporti contenenti dati personali non vengano allontanati dai luoghi ove si estrinseca il trattamento dei dati personali se da essi non vengono eliminati e/o cancellati tutti i dati in essi presenti.
Questo test muove anche dalla specifica conoscenza che i supporti magnetici possono essere cancellati in vari modi e che comunque un solo modo garantisce in maniera sicura e certa la detta cancellazione.
Tale modo è la sovrascrittura cui si farà particolare attenzione di apporre qualora un supporto dovrà essere riutilizzato. Il supporto magnetico eventualmente riscritto sarà riutilizzato solo ed esclusivamente dall'incaricato che lo utilizzava in precedenza e ciò al fine di evitare che uno stesso supporto venga impiegato per trattamenti diversi aventi finalità diverse e condotti da incaricati aventi autorizzazioni differenziate, quindi per evitare integralmente il rischio di lettura e/o di consultazione del supporto da parte di altri soggetti nel caso in cui il supporto non dovesse eventualmente essere riscritto nella sua interezza.
Per quel che attiene i documenti cartacei, questi saranno distrutti o resi illeggibili con apposite macchine distruggi documenti.

Al fine della corretta e puntuale applicazione delle prescrizioni imposte sono previsti, pertanto, dei controlli a campione a cura dei singoli Responsabili del Trattamento dei dati personali consistenti nella verifica occasionale del contenuto dei cestini, del contenuto dei supporti magnetici per la verificazione dell'eventuale grado di cancellazione e sovrascrittura. L'effettuazione di tale test e dei risultati ad esso sottesi deve essere menzionata ed inserita nell'aggiornamento del successivo Documento Programmatico sulla Sicurezza ed i punti critici eventualmente riscontrati posti alla base delle necessarie ed indefettibili modifiche che dovranno essere apportate al nuovo piano di sicurezza del trattamento dei dati personali.

8.5 TEST DI VERIFICA DELLE PROCEDURE DI GESTIONE DELLE PAROLE CHIAVE E DEI PROFILI DI AUTORIZZAZIONE DEGLI INCARICATI

Con tale test sarà verificata la corretta e puntuale osservanza dell'utilizzo delle password e delle user-id nonché la conoscenza da parte di tutti gli incaricati del trattamento delle procedure di scelta, modifica ed utilizzo delle parole chiave.
Tale verifica deve essere effettuata a campione dal responsabile del Trattamento dei dati personali il quale avrà cura, inoltre, di verificare anche la congruità e l'aggiornamento delle autorizzazioni all'accesso ed al trattamento dei dati.
Tali controlli dovranno essere anche effettuati in base al cambio di mansioni eventualmente assegnato ai singoli incaricati del trattamento.
L'effettuazione di tale test e dei risultati ad esso sottesi deve essere menzionata ed inserita nell'aggiornamento del successivo Documento Programmatico sulla Sicurezza ed i punti critici eventualmente riscontrati posti alla base delle necessarie ed indefettibili modifiche che dovranno essere apportate al nuovo piano di sicurezza del trattamento dei dati personali.

8.6 TEST DI VERIFICA DELLE PROCEDURE RELATIVE ALL'INTEGRITÀ E ALL'AGGIORNAMENTO DEI DATI PERSONALI

Con tale test si tende a verificare l'integrità e l'aggiornamento dei dati personali.
In particolare per quel che attiene l'integrità dei dati è necessario verificare la corrispondenza integrale del dato tra il momento della raccolta con quello del successivo momento del trattamento stesso.
Per quel che attiene l'aggiornamento del dato è necessario, invece, verificare la corrispondenza integrale del dato inizialmente conferito con quello da aggiornarsi anche in base ad una richiesta di aggiornamento da parte dell'interessato.
Contestualmente a detto controllo dovrà prevedersi inoltre una verifica in ordine all'efficienza delle procedure di backup dei dati automatizzati nonché dei tempi e della tempestività dell'aggiornamento dei dati in base alle comunicazioni inoltrate nell'Ente. I risultati di tale controllo debbono essere menzionati ed inseriti nell'aggiornamento del successivo Documento Programmatico sulla Sicurezza ed i punti critici eventualmente riscontrati posti alla base delle necessarie ed indefettibili

modifiche che dovranno essere apportate al nuovo piano di sicurezza del trattamento dei dati personali.

8.7 TEST DI VERIFICA DELLE MODALITÀ DI CONSERVAZIONE DEI DOCUMENTI

Questo test deve essere condotto sui documenti cd. cartacei che contengono dati personali e mira specificamente alla verifica delle procedure di conservazione di dati personali in generale e dei dati sensibili in particolare con controlli di efficienza delle condizioni dei contenitori muniti di serratura in cui i documenti sono conservati.
Questo controllo muove dalla considerazione che la legge impone la conservazione dei detti documenti all'interno di contenitori muniti di serratura e che gli stessi debbono essere chiusi a chiave. Pertanto, si procederà a controlli a sorpresa a cura dei Responsabili del Trattamento con particolare attenzione anche che le relative chiavi siano in possesso dei soli soggetti incaricati ed autorizzati per i singoli dati, che non esistano duplicati delle medesime chiavi, che vi siano chiavi di riserva e che le stesse siano correttamente conservate e custodite.
L'effettuazione di tale test e dei risultati ad esso sottesi deve essere menzionata ed inserita nell'aggiornamento del successivo Documento Programmatico sulla Sicurezza ed i punti critici eventualmente riscontrati posti alla base delle necessarie ed indefettibili modifiche che dovranno essere apportate al nuovo piano di sicurezza del trattamento dei dati personali.

8.8 TEST DI VERIFICA DEL LIVELLO DI FORMAZIONE E DEL GRADO DI APPRENDIMENTO DEGLI INCARICATI

Dopo avere affrontato nel capitolo 5 il piano di formazione degli incaricati del trattamento, sempre per le medesime ragioni in esso specificate, i Dirigenti di Settore prevedono questo ulteriore ed ultimo test di controllo del grado di apprendimento e di applicazione delle prescrizioni impartite e ciò in quanto hanno concordemente ritenuto che la formazione potrà dirsi ed affermarsi veramente tale solo ed esclusivamente se i suoi contenuti sono stati effettivamente recepiti e, quindi, applicati dai singoli incaricati del trattamento dei dati personali.
Per il raggiungimento di questo risultato il responsabile del Trattamento avrà cura di sottoporre un breve questionario di controllo ai singoli incaricati che hanno manifestato insufficienze di tipo applicativo.
Inoltre, a completamento del grado di formazione degli incaricati debbono inoltre prevedersi interviste personali anche in occasione dell'effettuazione della normale attività lavorativa e, poiché la formazione è un processo permanente, quanto riportato deve essere ripetuto ad intervalli irregolari.
I risultati di tale controllo debbono essere menzionati ed inseriti nell'aggiornamento del successivo Documento Programmatico sulla Sicurezza ed i punti critici eventualmente riscontrati posti alla base delle necessarie ed indefettibili modifiche che dovranno essere apportate al nuovo piano di sicurezza del trattamento dei dati personali.

SOTTOSCRIZIONE

La sottoscrizione del presente documento implica la piena scienza e coscienza del contenuto dello stesso. Ciascun Dirigente è tenuto ad attenersi scrupolosamente alle direttive indicate nel documento e avrà l'onere di notificarlo ai Responsabili e incaricati di Settore . La sottoscrizione qui di seguito apposta vale anche come ricevuta del documento informativo e delle istruzioni operative indicate nell'allegato C del presente documento.

IL DIRIGENTE DEL SETTORE 1°	**Dott. Francesco Lumiera**
IL DIRIGENTE DEL SETTORE 2°	**Dott. Michele Busacca**
IL DIRIGENTE DEL SETTORE 3°	**Dott. Salvatore Grande**
IL DIRIGENTE DEL SETTORE 4°	**Dott.ssa Orazia Parrino**
IL DIRIGENTE DEL SETTORE 5°	**Dott.ssa Nunzia Occhipinti**
IL DIRIGENTE DEL SETTORE 6°	**Avv. Angelo Frediani**
IL DIRIGENTE DEL SETTORE 7°	**Arch. Ennio Torrieri**
IL DIRIGENTE DEL SETTORE 8°	**Arch. Giorgio Colosi**
IL DIRIGENTE DEL SETTORE 9°	**Ing. Michele Scarpulla**
IL DIRIGENTE DEL SETTORE 10°	**Ing. Giulio Lettica**
IL DIRIGENTE DEL SETTORE 11°	**Dott. Giuseppe Mirabelli**
IL DIRIGENTE DEL SETTORE 12°	**Dott. Alessandro Licitra**
IL DIRIGENTE DEL SETTORE 13°	**Dott. Santi Di Stefano**
IL DIRIGENTE DEL SETTORE 14°	**Dott. Rodolfo Turrisi**
IL DIRIGENTE DEL SETTORE 15°	**Dott. Salvatore Scifo**