Serv. Determinazioni Dirigenziali
Trasmessa: Sett. I
Rag. Albo
il 02-08-2010
Il Resp. del servizio
L'Istruttore Amministrativo

SETTORE I
DETERMINAZIONE DIRIGENZIALE

Annotata al registro generale **In data** 31.03.2010 **n.** 595 **N.** 86 **Settore I** **data** 31.03.2010	**OGGETTO:** *Approvazione documento programmatico sulla Sicurezza (D.Lgs. n. 196/2003 e successive modifiche ed integrazioni).*

DIMOSTRAZIONE DELLA DISPONIBILITA' DEI FONDI

BIL. **CAP.** **FUNZ.**

SERV. **INT.** **IMP...../**

IL RAGIONIERE CAPO

L'anno duemiladieci,il giorno TRENTUNO del mese di MARZO, nell'ufficio del Settore I, il Dirigente, Dott. Francesco Lumiera, ha adottato la seguente determinazione:

Premesso che il decreto Legislativo 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 ultimi anni, e delle quali si dà atto all'interno del piano che è parte integrante e sostanziale del presente provvedimento;
che con determinazione sindacale n. 44 del 31.03.2009 è stato approvato il Documento programmatico sulla sicurezza dei dati personali, a modifica di quelli dei precedenti anni;
ritenuta la necessità di dovere aggiornare entro la data del 31.03.2010 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;
considerato che il presente atto non comporta alcun impegno di spesa;
Ritenuto che la materia di che trattasi rientra nelle competenze del Dirigente di Settore ai sensi dell'art. 53 del Regolamento di Organizzazione degli Uffici e dei Servizi comunali;
Vista l'attestazione della copertura finanziaria da parte del Capo settore Ragioneria ;
Ritenuto di dovere provvedere in merito;

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 ed delle disposizioni in esso previste;
3) Dare atto che il presente provvedimento non comporta impegno di spesa.

IL DIRIGENTE
(dott. Francesco Lumiera)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI PARTE INTEGRANTE

Da trasmettersi d'ufficio,oltre al Sindaco ed al Segretario Generale , ai seguenti settori\uffici:

Visto:

Il Dirigente del I Settore il Segretario Generale

Ragusa, li

IL Dirigente
Dr. Francesco Lumiera

Per presa visione:

Il Direttore Generale **Il Sindaco**

Ragusa, li

SETTORE SERVIZI CONTABILI E FINANZIARI

Visto per la regolarità contabile attestante la copertura finanziaria ai sensi dell'art. 151,4°comma,del TUEL

RAGUSA

IL RESPONSABILE DI RAGIONERIA

Il sottoscritto Messo comunale attesta di avere pubblicato in data odierna, all'Albo Pretorio, per la durata di giorni sette, copia della stessa determinazione dirigenziale, e di averne trasmesso copia, al Segretario Generale.

Ragusa 03 AGO. 2010

IL MESSO COMUNALE
IL MESSO NOTIFICATORE
(Licitra Giovanni)

Il sottoscritto Messo comunale attesta il compimento del suindicato periodo di pubblicazione e cioè dal 03 AGO. 2010 **al** 09 AGO. 2010

Ragusa 11 AGO. 2010

IL MESSO COMUNALE

---

n. 31 fascicolo

N. 595 del 31-03-2010

CITTÀ DI RAGUSA

www.comune.ragusa.it

SETTORE I – ASSISTENZA AGLI ORGANI ISTITUZIONALI, AFFARI GENERALI TURISMO

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 2010

DOCUMENTO APPROVATO CON DETERMINAZIONE DIRIGENZIALE N. .....595..... DEL 31-03-2010

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 responsabili 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 il 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. Ad integrazione di ciò è stato predisposto anche un regolamento specifico per la gestione dei dati provenienti dalla videosorveglianza, adottato con deliberazione di consiglio n. 6 del 10 febbraio 2009.

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, Via San Vito;
D) Settore IV, Corso Italia, 72;
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, Zona Artigianale e sedi decentrate;
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) Staff del Segretario Generale.

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 2010.

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 continuata 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 3 del presente documento.

IL DIRIGENTE DEL SETTORE 1°	**f.to Dott. Francesco Lumiera**
IL DIRIGENTE DEL SETTORE 2°	**f.to Dott. Michele Busacca**
IL DIRIGENTE DEL SETTORE 3°	**f.to Dott.ssa Cettina Pagoto**
IL DIRIGENTE DEL SETTORE 4°	**f.to Dott. Salvatore Scifo**
IL DIRIGENTE DEL SETTORE 5°	**f.to Dott. Giuseppe Mirabelli**
IL DIRIGENTE DEL SETTORE 6°	**f.to Avv. Angelo Frediani**
IL DIRIGENTE DEL SETTORE 7°	**f.to Arch. Ennio Torrieri**
IL DIRIGENTE DEL SETTORE 8°	**f.to Arch. Giorgio Colosi**
IL DIRIGENTE DEL SETTORE 9°	**f.to Ing. Michele Scarpulla**
IL DIRIGENTE DEL SETTORE 10°	**f.to Ing. Giulio Lettica**
IL DIRIGENTE DEL SETTORE 11°	**f.to Dott. Santi Di Stefano**
IL DIRIGENTE DEL SETTORE 12°	**f.to Dott. Alessandro Licitra**
IL DIRIGENTE DEL SETTORE 13°	**f.to Dott.ssa Elide Ingallina**
IL DIRIGENTE DEL SETTORE 14°	**f.to Dott. Rosario Spata**
IL SEGRETARIO GENERALE	**f.to Dott. Benedetto Buscema**

VADEMECUM ESPLICATIVO DEL TRATTAMENTO

(ISTRUZIONI OPERATIVE)

Al fine di gestire correttamente gli adempimenti connessi al D.Lgs 30 giugno 2003 n.196 "Testo Unico in materia di protezione dei dati personali", nonché per creare e sostenere la cultura della privacy all'interno dell'Ente, è stato elaborato il presente "Vademecum Esplicativo del Trattamento" che deve essere periodicamente aggiornato sia in base alle scadenze previste dalla legge sia in occasione di rilievi conseguenti a novità delle modalità del trattamento dei dati.
Il vademecum è uno strumento operativo e di dettaglio per la tutela della riservatezza dei dati personali in attuazione dei contenuti generali del regolamento comunale, e costituisce altresì la traduzione esecutiva del medesimo in rapporto all'assetto organizzativo nel tempo vigente come definito dalla Giunta Municipale mediante la dotazione organica, il regolamento sull'ordinamento degli uffici di servizi. In rapporto all'assetto organizzativo dell'Ente, costituisce parte integrante ed inscindibile del Documento Programmatico sulla Sicurezza.
Compito del presente documento è quello di individuare, descrivere e definire:le Responsabilità, nonché le istruzioni impartite ai soggetti preposti al Trattamento; le linee generali delle azioni necessarie per il monitoraggio del processo del trattamento dei dati personali in base ad una preventiva e dettagliata analisi dei rischi volta all'individuazione ed alla consequenziale adozione delle misure minime di sicurezza, ai sensi degli artt. da 33 a 36 del D.Lgs. 196/03; gli adempimenti necessari, sia a rilevanza cd. interna che esterna i quali ultimi sono evidenziati nel capitolo 5 del Vademecum Esplicativo del Trattamento.

0.2. RIFERIMENTI NORMATIVI

Artt. 2-4-5 D.Lgs. 196/03 Finalità, definizioni e campo di applicazione
Art. 11-7 D.Lgs. 196/03 Modalità del trattamento e requisiti dei dati
Artt. 18/19/20/21/22 D.Lgs. 196/03 Regole ulteriori per i soggetti pubblici
Artt. 20/22/26/62/95/107 D.Lgs. 196/03 Dati sensibili

0.3 STRUTTURA E GESTIONE DEL VADEMECUM ESPLICATIVO DEL TRATTAMENTO

Il presente Vademecum è strutturato in sezioni. Ogni sezione presenta degli allegati, che sono contrassegnati con la sigla VET/ALL. Le Sezioni sono numerate in ordine progressivo: da 00 a "0X". Gli Allegati sono individuati in modo univoco con la sigla VET/ALL seguita da due coppie di numeri (es. VET/ALL 05.01): la prima coppia fa riferimento alla Sezione del Vademecum Esplicativo del Trattamento; la seconda coppia il numero progressivo del documento, qualora una sezione presenti più di un allegato. Sulla copertina oltre all'indice generale è riportata una tabella che evidenzia lo stato delle verifiche da effettuarsi a cura del Gruppo Privacy, nel caso in cui verrà costituito e formalizzato un gruppo di lavoro, composto dai dai Dirigenti di Settore, e l'approvazione delle eventuali modifiche da adottarsi a cura del: Consiglio Comunale per l'eventuale adozione o modifica del regolamento generale per il Trattamento dei dati personali; Giunta con riferimento agli aspetti organizzativi, tra questi compresi i provvedimenti tendenti all'adozione delle misure minime di sicurezza.
Il presente deve essere tenuto ed aggiornato dal Gruppo Privacy che cura: la revisione periodica, formulando le proposte di modificazione e integrazione ai superiori organi che potranno provvedere alla loro approvazione; la corretta applicazione e conservazione del vademecum esplicativo del trattamento unitamente all'aggiornamento annuale del Documento Programmatico sulla Sicurezza; la distribuzione, anche per via telematica.
Lo stato di revisione del documento è riportato in alto, nella griglia di intestazione,contraddistinto da un numero progressivo e dalla data di approvazione.

0.4 D.LGS. 30 GIUGNO 2003 N.196: TESTO UNICO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Per una corretta, puntuale ed analitica applicazione delle norme di cui al citato Testo Unico in

materia di protezione dei dati personali si riportano le principali definizioni dalla cui riflessione possono discendere utili elementi interpretativi per l'applicazione dei vari adempimenti.

Trattamento si intende qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati.

Ai sensi dell'art. 3 del D. Lgs 196/03, i sistemi informativi devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o, rispettivamente, opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Dato personale si intende qualunque informazione relativa ad una persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati identificativi si intendono i dati personali che permettono l'identificazione diretta dell'interessato.

Dati sensibili sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. Ai sensi dell'art. 22 comma 6 e 7, i dati sensibili e giudiziari contenuti in elenchi, registri o banche dati tenuti con l'ausilio di strumenti elettronici sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare l'interessato solo in caso di necessità.

INTRODUZIONE GENERALE

I dati idonei a rivelare lo stato di salute e la vita sessuale, qualora trattati nell'ambito dell'ente comunale, sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Dati giudiziari, i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lett. da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n.313 in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Anche per i dati giudiziari, come per quelli sensibili, condizione di legittimità per il loro utilizzo è l'individuazione delle finalità di rilevante interesse pubblico, nonché i tipi di dati e le operazioni eseguibili

Dati comuni, non espressamente definiti dal legislatore. Costituiscono una categoria residuale, ricavabile per esclusione rispetto alle elencazioni tassative, di cui ai punti precedenti.

Banca dati, qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati, tali da facilitarne il Trattamento. La banca dati può assumere forme diverse: elenco di dari personali memorizzati in formato elettronico, schede relative a soggetti titolari dei dati identificativi, banche date cartacee costituite da fascicoli e cartelle ecc.

Titolare, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro

ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità e alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Tale figura è individuata nell'ambito dell'ente comunale nella figura dei Dirigenti di Settore.
Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposti dal Titolare al Trattamento di dati personali. Questa figura, che solitamente viene individuata nei soggetti posti al vertice dei singoli settori amministrativi dell'ente comunale, deve avere particolari requisiti di affidabilità, capacità e professionalità in quanto i compiti affidatigli presuppongono un alto grado di conoscenzadella materia.
Incaricati del Trattamento: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile.
Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti.
Sistema di autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità o della dichiarazione di identità.
Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati dal sistema di autenticazione informatica
per la verifica dell'identità o della dichiarazione di identità.
Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Profilo di autorizzazione: l'insieme dei dati cui una persona può accedere, nonché dei trattamenti ad essa consentiti.
Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Si ricordi comunque che i dati personali non sono solamente le informazioni cd. alfanumeriche, ma tutte quelle che si riferiscono ad un soggetto, comunque identificabile: la nozione è volutamente molto ampia, poiché ricomprende anche immagini e suoni (si pensi alla videosorveglianza e alle audioregistrazioni, che costituiscono modalità di Trattamento dei dati personali).
La legge detta una serie di regole procedurali per garantire la tutela delle persone e di altri soggetti da questa attività.
Ovvio che a seconda della natura dei dati trattati muteranno le regole e le cautele previste, anche in considerazione della maggiore o minore invasività della sfera più intima degli interessati.
In particolare, per intendere realmente il campo di applicazione della legge e soprattutto il fatto che soggetto destinatario della tutela e della relativa protezione è l'interessato i cui dati sono trattati dal Titolare del Trattamento, si ritiene fondamentale, infatti, riportare i capisaldi del D.Lgs. 196/03 costituiti dagli articoli 11 e 7 contenenti una serie di disposizioni riferite alla garanzia di qualità e ai controlli sul processo di Trattamento:
l'art. 11 introduce vari principi generali in riferimento al trattamento dei dati personali ed in particolare alla necessità che gli stessi siano esatti e aggiornati, nonché pertinenti, completi e

non eccedenti rispetto alle finalità. Le modalità di svolgimento delle operazioni di Trattamento devono essere svolte in modo lecito e secondo correttezza, nonché per scopi determinati, espliciti e legittimi;
l'art. 7 elenca una serie di diritti riconosciuti all'interessato: dal diritto di ottenere dal titolare del trattamento la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, nonché la loro comunicazione in forma intelligibile. Inoltre la legge riconosce al soggetto cui si riferiscono i dati personali la possibilità di esercitare una serie di poteri sia di carattere inibitorio, sia cd. integrativi, quali ad esempio la richiesta di cancellazione, trasformazione in forma anonima o il blocco dei dati, in caso di violazione di legge, ovvero l'aggiornamento, la rettificazione o l'integrazione dei dati, fino all'opposizione al Trattamento, per motivi legittimi.

0.5. CAMPO D'APPLICAZIONE DEL D. LGS 196/03 (ART. 5)

Il Testo Unico disciplina il trattamento dei dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla Sovranità dello Stato o chiunque è stabilito nel territorio di un Paese non appartenente all'Unione Europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato.
Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del Codice della Privacy solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni dell'art. 15 (danni cagionati per effetto del trattamento) e dell'art. 31 (misure minime di sicurezza).
Per i trattamenti svolti da Enti Pubblici, oltre le norme generali contemplate negli artt. 11 – 17 del Testo Unico, sono previste alcune regole specifiche; in particolare: E' consentito solo per lo svolgimento di funzioni istituzionali; Devono essere osservati i presupposti e i limiti stabiliti dal Testo Unico, dalla legge e dai regolamenti; Salvo che per le professioni sanitarie e gli organismi sanitari Pubblici , gli Enti Pubblici non devono richiedere il CONSENSO dell'interessato, pur dovendo informare l'interessato del trattamento dei dati che sarà posto in essere dall'ente; Si applica l'art. 25 in tema di comunicazione e diffusione;
Il trattamento dei dati diversi da quelli sensibili e giudiziari (dati comuni) è consentito anche in mancanza di una norma di legge o regolamento che lo preveda espressamente; la comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o regolamento: In mancanza è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali; la comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o regolamento.
Il trattamento dei dati sensibili e giudiziari: E' consentito solo se autorizzato dalla legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite; qualora in essa non siano specificati i dati sensibili e le operazioni eseguibili, il trattamento è consentito solo per quei tipi di dati e di operazioni identificati e resi pubblici dai soggetti che ne effettuano il trattamento con atto di natura regolamentare adottato in conformità al parere espresso dal Garante; in alternativa possono chiedere al Garante l'individuazione delle attività, tra quelle affidate ai medesimi soggetti dalla legge, per le quali è autorizzato al trattamento dei dati.

0.6. IL GARANTE PER LA PRIVACY

Il Garante per la protezione dei dati personali è organo indipendente la cui sede si trova in Roma, Piazza Monte Citorio n° 121. E' composto da quattro membri che durano in carica quattro anni.

Il Garante ha il compito di controllare la conformità dei trattamenti di dati personali alle disposizioni in materia di privacy ed eventualmente vietare i trattamenti illeciti, esaminare ricorsi e reclami che gli siano pervenuti, denunciare i fatti configurabili come reato di cui sia venuto a conoscenza nell'esercizio delle sue funzioni, tenere il registro dei trattamenti soggetti a notificazione ecc. E' possibile porre quesiti e chiedere chiarimenti all'ufficio del Garante telefonando al n° 06 69677917. Ulteriori informazioni e aggiornamenti in materia di Privacy possono essere fornite collegandosi al sito www.garanteprivacy.it .

1) FINALITA' DI RILEVANTE INTERESSE PUBBLICO CONTENUTE NEL D. LGS 196/03

MODALITA' DI RICOGNIZIONE DELLE BANCHE DATI E DEI TRATTAMENTI AL FINE DEL CONFRONTO CON LE FINALITA' DI RILEVANTE INTERESSE PUBBLICO

SCOPO

Scopo del presente capitolo è quello di individuare quali sono i trattamenti, fra quelli di pertinenza di un ente comunale che, in quanto ritenuti di rilevante interesse pubblico, sono già stati autorizzati dalle legge.

L'elenco delle finalità sotto riportate ha lo scopo di consentire il confronto con le banche dati trattate dal Comune di Ragusa al fine di verificare se tutte rientrino oppure no nell'ambito delle finalità già previste ed autorizzate dalla legge.

A tal fine è stata individuata una particolare procedura di ricognizione delle banche dati trattate da codesto ente.

Ciò non vuol dire che l'elenco delle finalità sotto riportate debba considerarsi esaustivo in quanto ben il Comune potrebbe effettuare trattamenti diversi da quelli di rilevante interesse pubblico già autorizzati dal legislatore.

Tuttavia, qualora il Comune di Ragusa individui ambiti di trattamento ulteriori rispetto a quelli già autorizzati, è necessario richiedere specifica autorizzazione al trattamento direttamente al Garante per la Privacy oppure approvare un regolamento comunale che specifichi le rilevanti finalità di interesse pubblico perseguite, le categorie di dati personali che possono essere trattati e i tipi di operazioni di trattamento eseguibili, ciò sulla base dei modelli predisposti dal Garante e scaricarli dal sito dell'ANCI (Associazione Nazionale Comuni Italiani).

1.2. RIFERIMENTI NORMATIVI

Artt. 18/19/20/21/22 D.Lgs. 196/03 Regole ulteriori per i soggetti pubblici
Artt. 20/22/26/62/95/107 D.Lgs. 196/03 Dati sensibili
Artt. 42/43/44/45 D.Lgs. 196/03 Trasferimento di dati personali all'estero
Artt. 59/60 D.Lgs. 196/03 Accesso a documenti amministrativi
Artt. 62/63 D.Lgs. 196/03 Stato civile, anagrafi e liste elettorali
Artt. 64/65/66/67/68/69/70/71
72/73
D.Lgs. 196/03
Finalità di rilevante interesse pubblico
Art. 74 D.Lgs. 196/03 Circolazione stradale

1.3.FINALITA' DI RILEVANTE INTERESSE PUBBLICO CONTENUTE NEL D.LGS 196/03

Preliminarmente è opportuno chiarire la differenza fra due concetti che sono spesso oggetto di

confusione e fraintendimenti. Si intende per "finalità di rilevante interesse pubblico" quelle finalità che la Pubblica Amministrazione persegue in quanto di interesse collettivo, che ineriscono cioè a tutti i soggetti.
L'interesse pubblico si caratterizza quindi perché i soggetti coinvolti e le attività svolte per il suo perseguimento sono sottoposti a particolari regolamentazione. Per la realizzazione dell'interesse pubblico l'ente titolare può essere dotato di poteri autoritativi.
Si intende invece per "funzioni istituzionali" l'ambito di quelle attività che istituzionalmente, in quanto demandate dalla legge, sono affidate allo svolgimento di quel particolare ente pubblico. Il dovere istituzionale dell'ente è quello di perseguire l'interesse collettivo.
Pertanto l'ente pubblico deve effettuare il trattamento dei dati personali non solo al fine esclusivo di perseguire l'interesse superiore dell'intera collettività, ma deve farlo nei limiti strettamente definiti dai compiti che la legge gli ha affidato. Il trattamento compiuto per una finalità diversa dall'interesse pubblico o nell'ambito di funzioni che spettano ad un altro ente è da ritenersi illegittimo.
Orbene, il Garante per la Privacy ha individuato nel corpo del D. Lgs 196/03, soprattutto nel testo del titolo IV, molte fra le finalità di interesse pubblico che la Pubblica Amministrazione, nell'ambito delle funzioni istituzionali attribuite ai singoli enti, può perseguire; ciò sia nell'ambito del trattamento dei dati comuni che di quelli sensibili.
Ad esempio, nell'art. 62 intitolato "dati sensibili e giudiziari", si fa riferimento alle finalità relative alla tenuta degli atti e dei registri dello stato civile, delle anagrafi e delle liste elettorali, nonché quelle relative al rilascio dei documenti di identità o al cambiamento di generalità.
Come già detto, il trattamento dei dati sensibili da parte di enti pubblici è consentito quanto è previsto da una norma di legge che specifichi le rilevanti finalità di interesse pubblico perseguite, le categorie di dati personali che possono essere trattati e i tipi di operazioni di trattamento eseguibili
Tutte e tre queste condizioni devono essere soddisfatte affinché il trattamento possa considerarsi legittimo. Ne consegue che, qualora una norma individui, ad es., solo le finalità di interesse pubblico ma non le categorie di dati trattabili e i tipi di operazioni eseguibili, sarà compito dell'ente pubblico provvedere, con atto di natura regolamentare, all'integrazione della norma. Ad esempio agli artt. 64 e 65 del D. Lgs 196/03 vengono individuate sia le finalità di rilevante interesse pubblico, sia i tipi di dati, sia le operazioni eseguibili (indicate con le lettere dell'alfabeto). Tuttavia non è sempre così. Al contrario l'art. 66 individua le finalità di rilevante interesse pubblico ma non i dati trattabili e le operazioni eseguibili rinviando così implicitamente all'atto di natura regolamentare adottato dall'ente pubblico.
Le finalità di rilevante interesse pubblico individuate dal T.U. D.LGS. 196/03 sono:
Finalità di applicazione della disciplina dell'accesso agli atti amministrativi.
In particolare, fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.(art. 59). Finalità relative alla tenuta degli atti e dei registri dello stato civile, anagrafi e liste elettorali, nonché rilascio dei documenti di riconoscimento o cambiamento delle generalità (art. 62) Finalità di applicazione della disciplina in materia di cittadinanza, immigrazione, asilo, e condizione dello straniero e del profugo e sullo stato di rifugiato. (art. 64) In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a: rinnovo dei visti, permessi, attestazioni, autorizzazioni e documenti sanitari; riconoscimento del diritto di asilo o dello stato di rifugiato, o all'applicazione della protezione temporanea o di altri istituti

o misure di carattere umanitario, ovvero all'attuazione di obblighi di legge in materia di politiche migratorie; in relazione agli obblighi dei datori di lavoro e dei lavoratori, ai ricongiungimenti, all'applicazione delle norme vigenti in materia di istruzione e di alloggio, alla partecipazione alla vita pubblica e all'integrazione sociale.
Finalità di applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio dei diritti politici nonché della pubblicità dell'attività di organi pubblici. (art. 65) In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a: elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonché di esercizio del mandato degli organi rappresentativi o di tenuta degli elenchi dei giudici popolari; b) documentazione dell'attività istituzionale di organi pubblici.
I trattamenti dei dati sensibili e giudiziari per le finalità di cui alla lettera a) sono consentiti per eseguire specifici compiti previsti da leggi o da regolamenti fra i quali, in particolare, quelli concernenti:
lo svolgimento di consultazioni elettorali e la verifica della relativa regolarità;
le richieste di referendum, le relative consultazioni e la verifica delle relative regolarità;
l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi;
l'esame di segnalazioni, petizioni, appelli e di proposte di legge di iniziativa popolare, l'attività di commissioni di inchiesta, il rapporto con gruppi politici;
la designazione e la nomina di rappresentanti in commissioni, enti e uffici.

Ai fini del presente articolo, è consentita la diffusione dei dati sensibili e giudiziari per le finalità di cui alla lettera a), in particolare con riguardo alle sottoscrizioni di liste, alla presentazione delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti.
Ai fini del presente articolo, in particolare, è consentito il trattamento di dati sensibili e giudiziari per la redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari; per l'esclusivo svolgimento di una funzione di controllo, di indirizzo politico o di sindacato ispettivo e per l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo.
- Finalità di applicazione della disciplina in materia tributaria e doganale.
In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a: applicazione, anche tramite i loro concessionari, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai responsabili di imposta, nonchè in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione è affidata alle dogane. attività dirette, in materia di imposte, alla prevenzione e repressione delle violazioni degli obblighi e alla adozione dei provvedimenti previsti da leggi, regolamenti o dalla normativa comunitaria, nonché al controllo e alla esecuzione forzata dell'esatto adempimento di tali obblighi, alla effettuazione dei rimborsi, alla destinazione di quote d'imposta, e quelle dirette alla gestione ed alienazione di immobili statali, all'inventario e alla qualificazione degli immobili e alla conservazione dei registri immobiliari. (art. 66)
- Finalità di applicazione della disciplina in materia di attività di controllo e ispettive.
In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a: verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti;
b) accertamento, nei limiti delle finalità istituzionali, con riferimento a dati sensibili e giudiziari relativi ad esposti e petizioni, ovvero ad atti di controllo o di sindacato ispettivo di cui all'articolo 65, comma 4. (art. 67)

Finalità di applicazione della disciplina in materia di concessione di benefici e abilitazioni. (art. 68)
In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a:
a) ammesso il trattamento di dati sensibili e giudiziari indispensabili a:
a) finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.
Si intendono compresi fra i trattamenti regolati dal presente articolo anche quelli indispensabili in relazione: alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia; alle elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive; alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti; al riconoscimento di benefici connessi all'invalidità civile; alla concessione di contributi in materia di formazione professionale; alla concessione di contributi,finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti; g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria.

- Finalità di applicazione della disciplina in materia di conferimento di onorificenze, ricompense e riconoscimenti.
In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili il trattamento di dati sensibili e giudiziari indispensabili all'applicazione della disciplina in materia di conferimento di onorificenze e ricompense, di riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonchè di rilascio e revoca di autorizzazioni o abilitazioni, di concessione di patrocini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali. (art. 69)
- Finalità di applicazione della disciplina in materia di rapporti tra soggetti pubblici e organizzazioni di volontariato
In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili per :
a) l'elargizione di contributi finalizzati al loro sostegno, la tenuta di registri generali delle medesime organizzazioni e la cooperazione internazionale. (art. 70.1)
b) Finalità di applicazione della legge 230/98 e delle altre disposizioni di legge in materia di obiezione di coscienza (art. 70.2)
- Finalità di applicazione della disciplina in materia di sanzioni amministrative e ricorsi nonché volte a far valere il diritto di difesa in sede amministrativa o giudiziaria. (art. 71)
In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a:
applicazione delle norme in materia di sanzioni amministrative e ricorsi;
b) volte a far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da parte di un terzo, anche ai sensi dell'articolo 391 quater del codice di procedura penale, o direttamente connesse alla riparazione di un errore giudiziario o in caso di violazione del termine ragionevole del processo o di un'ingiusta restrizione della libertà personale.
Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito solo se il diritto da far valere o difendere è di rango almeno pari a quello dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale inviolabile.
- Finalità relative allo svolgimento dei rapporti istituzionali con enti di culto e confessioni o comunità religiose (art. 72)

- Finalità relative ad attività che la legge demanda ad un soggetto pubblico, le finalità socio-assistenziali.

In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a: interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare; interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto; assistenza nei confronti di minori, anche in relazione a vicende giudiziarie; indagini psico-sociali relative a provvedimenti di adozione anche internazionale; compiti di vigilanza per affidamenti temporanei; iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi; interventi in tema di barriere architettoniche.

Inoltre: a) di gestione di asili nido; b) concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico; c) ricreative o di promozione della cultura e dello sport, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico; d) di assegnazione di alloggi di edilizia residenziale pubblica; e) relative alla leva militare; f) di polizia amministrativa anche locale, salvo quanto previsto dall'articolo 53, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente, tutela delle risorse idriche e difesa del suolo; g) degli uffici per le relazioni con il pubblico; h) in materia di protezione civile; i) di supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro; l) dei difensori civici regionali e locali.

- Finalità relative alle attività amministrative correlate all'applicazione della disciplina sulla tutela sociale della maternità e interruzione volontaria di gravidanza, stupefacenti e sostanze psicotrope, di assistenza, integrazione sociale e diritti degli handicappati (art. 86).

In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a: tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonchè per gli interventi di interruzione della gravidanza; stupefacenti e sostanze psicotrope, con particolare riferimento a quelle svolte al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti, gli interventi anche di tipo preventivo previsti dalle leggi e l'applicazione delle misure amministrative previste;assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di:1) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni; 2) curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge; 3) realizzare comunita-alloggio e centri socio riabilitativi; 4) curare la tenuta degli albi degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore.

- Finalità di istruzione e di formazione in ambito scolastico o universitario (art. 95)
- Finalità relative ai trattamenti per scopi storici e relative ai trattamenti del SISTAN (art. 98)
- Finalità di instaurazione e gestione dei rapporti di lavoro di ogni tipo da parte degli enti pubblici e di collocamento obbligatorio (art. 112).

In particolare è ammesso il trattamento di dati sensibili e giudiziari indispensabili a:

Instaurazione di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.

Tra i trattamenti effettuati per le finalità di cui sopra, si intendono ricompresi, in particolare, quelli effettuati al fine di: a) applicare la normativa in materia di collocamento obbligatorio e

assumere personale anche appartenente a categorie protette; b) garantire le pari opportunità; c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni; d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali; e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale; f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente; g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare ricorsi amministrativi in conformità alle norme che regolano le rispettive materie; h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro; i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi; l) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti; m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale; n) svolgere l'attività di indagine e ispezione presso soggetti pubblici; o) valutare la qualità dei servizi resi e dei risultati conseguiti.

1.4. MODALITA' DI RICOGNIZIONE DELLE BANCHE DATI E DEI TRATTAMENTI AL FINE DEL CONFRONTO CON LE FINALITA' DI RILEVANTE INTERESSE PUBBLICO

Per la legittimità del trattamento è necessario che il soggetto pubblico provveda ad individuare le categorie di dati e le operazioni eseguibili mediante un'apposita procedura ricognitiva finalizzata al confronto dei dati con i parametri forniti dalla legge.

Questa ricognizione, da aggiornarsi periodicamente, è necessaria anche al fine di confrontare i trattamenti effettuati con quelle finalità di rilevante interesse pubblico per le quali esiste una specifica base normativa ma manchi l'individuazione dei dati e delle operazioni eseguibili. In tali casi è necessario che l'ente provveda a colmare i vuoti legislativi con regolamento interno che individui i dati e le operazioni eseguibili.

E' compito imprescindibile dell'Ente Comunale effettuare il continuo monitoraggio della corrispondenza dei trattamenti effettuati con quelli previsti e autorizzati dalla legge al fine di provvedere immediatamente all'adozione delle misure idonee atte a garantire la legittimità del trattamento.

La procedura di ricognizione delle banche dati e dei trattamenti effettuati dall'ente comunale, Titolare del Trattamento, si è sviluppata secondo le seguenti fasi:

Ricognizione delle banche dati e dei trattamenti che il soggetto pubblico intende proseguire in relazione alle attività di interesse pubblico sopra individuate.

A tal fine, presentando l'ente comunale una struttura particolarmente complessa, la ricognizione è stata eseguita mediante la compilazione e sottoscrizione di apposite schede da parte dei singoli incaricati del trattamento.

Valutazione della pertinenza e necessità dei dati e delle operazioni rispetto alle suddette finalità.
Descrizione del contenuto nell'ambito del Documento programmatico sulla sicurezza.

2) GRUPPO PRIVACY

2.1. SCOPO E RESPONSABILITA'
2.2. DESCRIZIONE
2.3 ALLEGATI

2.1 SCOPO E RESPONSABILITÀ'

Il Gruppo Privacy non è un organo espressamente previsto dal D.Lgs. 196/03.
Tuttavia, considerato l'impatto trasversale della Legge sulla Privacy e la necessità di procedere ad una serie di adempimenti, sia a rilevanza cd. interna, sia esterna, l'Ente può ritenere opportuno di procedere alla sua costituzione, con determinazione sindacale.
Spetterà al Sindaco, in qualità di rappresentante legale dell'Ente, Titolare del Trattamento, ai sensi dell'art. 28 del D.Lgs.196/03 , anche attraverso un suo delegato, presiedere, coordinare, controllare e convocare il Gruppo Privacy.
Ai sensi dell'art. 28 "quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico del tutto autonomo che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza".

2.2 DESCRIZIONE

Nell'eventualità in cui l'Ente vorrà procedere alla costituzione del Gruppo Privacy, questo deve essere il primo adempimento che deve compiere dopo l'approvazione del presente Vademecum Esplicativo del Trattamento e del Documento Programmatico sulla Sicurezza.
Il gruppo privacy può essere costituto da soggetti aventi diverse professionalità:
personale/dirigente amministrativo: soggetti che hanno una qualificata formazione giuridica e conoscono gli adempimenti generali sull'applicabilità e rispetto del D.Lgs. 196/2003, nonché la normativa specifica di settore, e funzionari ai quali sono stati assegnati incarichi particolari in relazione all'applicazione della legge sulla privacy. In tal caso possono costituire il gruppo privacy tutti i Responsabili pro tempore di ciascuna Area Amministrativa insieme ai responsabili di Servizio, in relazione alla dotazione organica dell'ente e all'ordinamento dei servizi e degli uffici.
personale con competenze gestionali: la legge ha un forte impatto trasversale e richiede la revisione di procedure e il monitoraggio dei flussi informativi in seno all'Ente e verso l'esterno.
Può essere utile quindi cogliere il valore aggiunto della legge sulla privacy in termini di riorganizzazione e di miglioramento dell'offerta dei propri servizi all'utenza; in questa ottica, fanno parte del Gruppo, in via necessaria i Responsabili di Area come individuati dal regolamento sull'ordinamento degli uffici e dei servizi, nei soggetti incaricati delle posizioni organizzative per i Servizi di competenza;
personale tecnico-informatico: sono il Responsabile dei servizi informatici e automatizzati e gli operatori del CED qualora presenti nell'Ente. Hanno una formazione tecnica e portano il loro contributo soprattutto in relazione alla valutazione dei rischi e all'adozione delle misure di sicurezza;
consulente Responsabile Audit Privacy: società di consulenza o libero professionista avente competenza giuridica e approfondita conoscenza sul D.Lgs. 196/03, nonché la normativa specifica di settore, sul controllo e sulle verifiche dell'operato dei Responsabili del Trattamento unitamente ad una generale funzione di indirizzo. Tale soggetto deve collaborare fattivamente con gli altri componenti del Gruppo Privacy anche con azioni di impulso

tendenti sia alla verifica delle procedure adottate dall'Ente che alla individuazione di nuove e più efficaci procedure di salvaguardia dei dati personali qualora si rinvenissero anomalie e/o disfunzioni nel Trattamento.
Al Gruppo Privacy verranno assegnati i seguenti compiti:
predisposizione delle schede da utilizzare per l'aggiornamento e controllo periodico del processo di trattamento al fine di monitorare l'insieme delle varie attività di Trattamento;
elaborazione dei dati raccolti presso le unità dell'Ente (aree, servizi, uffici) con le schede, di cui in allegato Documento programmatico Sulla Sicurezza;
segnalazione agli organi competenti delle azioni necessarie;
valutazione delle misure minime di sicurezza ritenute necessarie, che vengono proposte alla Giunta Municipale che provvederà alla loro adozione ed approvazione;
predisposizione dei moduli per le informative agli interessati;
programmazione di attività di formazione diretta e di informazione del personale preposto allo svolgimento delle operazioni di Trattamento;
cura e aggiornamento del presente Vademecum unitamente al Documento Programmatico sulla Sicurezza (DPS) ;
distribuzione del VET, del DPS e degli allegati in esso contenuti, utilizzando anche strumenti telematici;
segnalazione delle innovazioni di carattere normativo e delle necessarie modificazioni da apportare al Documento Programmatico sulla Sicurezza e alla modulistica allegata;
effettuazione di attività di audit e di controllo sulla rispondenza delle attività svolte rispetto a quanto previsto dalla legge e dalla documentazione dell'Ente;
revisione periodica della modulistica;
raccolta di quesiti di interesse sulla materia della privacy;
controllo sulle richieste di accesso da parte degli interessati e sul soddisfacimento dei diritti previsti dall'art. 7 del D.Lgs.196/03;
relazione periodica sulle attività di Trattamento;
Comunicazione al Sindaco in qualità di rappresentante dell'Ente Titolare del Trattamento, dell'aggiornamento periodico della lista degli incaricati del trattamento dei dati personali.
PER QUANTO SOPRA IL GRUPPO PRIVACY COSTITUISCE LO STRUMENTO PER FAVORIRE IL CONFRONTO E
LO SCAMBIO DI OPINIONI E DI ESPERIENZE IN MATERIA DI PRIVACY E DI SICUREZZA.

2.3 ALLEGATI

Copia determinazione "Costituzione e nomina Gruppo Privacy"

3) MONITORAGGIO DEL PROCESSO DI TRATTAMENTO

3.1. SCOPO

Scopo della presente sezione è descrivere le fasi del processo di Trattamento dei dati personali e le azioni di monitoraggio dello stesso, al fine della predisposizione degli adempimenti necessari aventi rilevanza sia interna che esterna.

3.2. RIFERIMENTI NORMATIVI

Articolo Norma	Descrizione
Art. 29 D.Lgs. 196/03	Responsabile del Trattamento
Art. 30 D.Lgs. 196/03	Incaricati del Trattamento
Artt. 25/39 D.Lgs. 196/03	Comunicazione e diffusione

3.3. RESPONSABILITÀ'

L'attività di monitoraggio del Trattamento dei dati personali è effettuata a cura del Gruppo Privacy e dei Responsabili del Trattamento, nominati ai sensi dell'art. 29 del D.Lgs.196/03 con idoneo documento allegato al DPS.
Le risultanze del Trattamento dei dati personali posti in essere dai singoli Responsabili dovranno essere regolarmente comunicate a cadenza periodica e, comunque, a cadenza almeno annuale al Gruppo Privacy.
Rimane salvo il diritto nonché l'obbligo di ogni Responsabile di chiedere al Sindaco o al suo delegato la convocazione del Gruppo Privacy qualora rinvenisse anomalie nel Trattamento dei dati affidati alla sua Responsabilità e/o qualora si verificassero situazioni di eccezionali gravità che ne impongono l'immediata convocazione, come la valutazione per l'adozione delle misure minime di sicurezza.

3.4. DESCRIZIONE

Il procedimento di Trattamento dei dati personali è caratterizzato da tre fasi:
INPUT - raccolta dati presso l'interessato o richiesta di comunicazione di dati personali a enti o persone giuridiche;
BLACK-BOX - (ossia il complesso delle operazioni di Trattamento interne);
OUTPUT - è la fase della comunicazione.

3.4.1. Le fasi del processo

La legge definisce il Trattamento di dati come qualunque operazione o complesso di operazioni svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la: Raccolta; Registrazione; Organizzazione; Conservazione; Elaborazione; Modificazione; Selezione; Estrazione; Raffronto; Utilizzo; Interconnessione; Blocco; Comunicazione; Diffusione; Cancellazione; Distruzione dati.
La raccolta dei dati può essere effettuata o direttamente presso l'interessato o presso terzi, che

conferiscono dati relativi a interessati diversi dalla propria persona (ad esempio, in tema di servizi socio – assistenziali a carico del Comune, la raccolta di dati da soggetti diversi da quelli cui il servizio erogato dall'Ente si riferisce. Es. familiari.)
E' necessario tenere ben presente che per osservare gli adempimenti connessi al trattamento dei dati personali, al momento della raccolta dei dati personali, occorre fornire all'interessato, presso il quale i dati sono raccolti, una esaustiva informativa, secondo quanto previsto dall'art. 13 del D.Lgs. 196/03.
Inoltre i soggetti pubblici, per poter trattare i dati personali, non devono ricevere il consenso da parte degli interessati.
La legge sulla privacy a tal proposito prevede due regimi di legittimazione diversi a seconda della natura dei soggetti titolari del Trattamento:
se a procedere al Trattamento è un soggetto privato (cui sono equiparati gli enti pubblici economici), questo deve chiedere preliminarmente il consenso all'interessato, salvo i casi di esclusione espressamente previsti dal legislatore;
per i soggetti pubblici, al contrario, vige il principio di finalità istituzionale (o secondo altri di competenza): essi possono trattare solo i dati che siano necessari per lo svolgimento di funzioni istituzionali.
Questa scelta è una conseguenza del principio di legalità, che caratterizza l'attività amministrativa, per cui si è voluto evitare di condizionare l'azione al consenso degli interessati. Peraltro questa scelta, fatta dal nostro legislatore, appare pienamente compatibile con quanto previsto, in sede comunitaria, dall'art. 7 della direttiva 95/46/CE.
Regola cardine per i soggetti pubblici è l'art.18 comma 2 "qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali".
La disposizione ha un duplice scopo, definire sia la giustificazione sia il limite del trattamento.
Altro punto importante riguarda il comma 3 dell'art.18, il soggetto pubblico nel trattare i dati osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla natura diversa dei dati, nonché dalla legge e dai regolamenti. Questa definizione ribadisce che la qualità soggettiva pubblica non assegna alcun potere speciale, occorre sempre una norma per poter svolgere le funzioni.
Il successivo comma 4 dell'art.18 introduce una norma di portata "operativa", scioglie ogni dubbio emerso in passato: il soggetto pubblico non deve chiedere il consenso all'interessato, salvo quanto previsto nella parte II per gli esercenti le attività sanitarie e gli organismi sanitari pubblici".
Ritornando all'attività di monitoraggio del processo di Trattamento, finalizzata a verificare "chi fa e come lo fa" e quindi ad avere un quadro completo sugli elementi caratterizzanti l'intero Trattamento, sono tre le fasi che lo caratterizzano.
Per quanto riguarda l'input non ci sono particolari problemi, salvo dover verificare se la raccolta di dati è necessaria per adempiere ad obblighi di legge oppure se è necessaria all'organizzazione aziendale.
Invece le operazioni di output, che costituiscono una species del genus Trattamento riguardano:
la comunicazione, ossia 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;
la diffusione, ossia il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
La differenza fra queste due operazioni è data dalla determinatezza o meno del soggetto destinatario delle informazioni: come è facile intuire queste due operazioni comportano i rischi maggiori per gli interessati.
Tanto è vero che la legge prevede che:

l'interessato deve essere informato sulle categorie di soggetti ai quali i dati possono essere comunicati e sull'ambito di diffusione dei dati medesimi; se i dati trattati sono comunicati da soggetto pubblico a altri soggetti pubblici, in questo caso la comunicazione è ammessa se prevista da espressa disposizione di legge o regolamento, in mancanza è ammessa solo nel caso in cui è necessaria per lo svolgimento di compiti istituzionali e può essere iniziata decorsi 45 giorni dalla comunicazione fatta al Garante.
la Comunicazione da soggetto pubblico a privati o diffusione da parte di soggetto pubblico, è ammessa solo se previsto da norma di legge o regolamento.
Se i dati trattati sono di natura sensibile per poter essere trasferiti occorre rispettivamente il consenso scritto dell'interessato, quando il Titolare sia un soggetto privato, una espressa autorizzazione di legge, nel caso dei soggetti pubblici.

3.4.2. Schede per il monitoraggio del processo di trattamento
Data la complessità organizzativa dell'Ente e considerati gli adempimenti previsti dal D.Lgs. 196/03 e il suo forte impatto trasversale, si è ritenuto indispensabile procedere ad una azione di monitoraggio delle attività di Trattamento svolte, al fine di avere un quadro generale e di verificare la compatibilità della situazione reale con le previsioni normative.
In particolare sono state predisposte ed utilizzate le seguenti schede per il monitoraggio distinte in relazione alle Aree Amministrative dell'Ente con riferimento a ciascun Servizio/ufficio.
Tali schede sono in allegato al Documento Programmatico Sulla Sicurezza.
Elenco Incaricati del Trattamento (DPS/ALL 01.01);
Scheda tecnica (DPS/ALL 02.01);
Scheda di processo (DPS/ALL 03.01).
Elenco incaricati: in questo allegato sono raccolti i dati nominativi, l'area di appartenenza, la funzione e le banche dati trattati da ogni soggetto in seno o per conto dell'Ente. Lo scopo è raccogliere una serie di dati e di informazioni, al fine della creazione dei profili degli incaricati del Trattamento;
scheda tecnica: si sono monitorate le risorse informatiche e telematiche utilizzate, in modo da avere il quadro completo degli strumenti utilizzati.
Inoltre sono state monitorate le banche dati costituite e detenute in seno all'Ente, sia con strumenti elettronici, sia in archivi cartacei. Lo scopo è quello di avere un quadro ben definito per l'adozione delle misure di sicurezza (così come riportate nel DPS);
scheda di processo: riguarda le tre fasi del Trattamento (come detto input - black-box e output). Si tratta di una ricognizione scrupolosa, in cui si evidenziano tutte le attività materiali che l'Ente persegue al fine di individuare: le finalità di Trattamento delle banche dati, ossia gli scopi, per cui i dati vengono raccolti e successivamente trattati. Si ricorda che l'art. 11 della D.Lgs.196/03 prevede che i fini devono essere determinati, espliciti e legittimi. Inoltre i dati possono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
le modalità di Trattamento, ossia gli strumenti che vengono utilizzati per trattare i dati (elettronici o comunque automatizzati, oppure cartacei) e la logica del Trattamento;
la natura dei dati trattati (comuni, sensibili o giudiziari): si è già ribadito, come la tipologia dei dati trattati influisca sulle specifiche regole di legittimazione al Trattamento;
l'ambito di comunicazione e diffusione. In questo caso lo scopo è duplice: verificare il flusso informativo dall'Ente verso l'esterno, monitorando le categorie di soggetti destinatari ovvero l'ambito di diffusione; monitorare le coperture normative, per le operazioni di output.
Inoltre ci sono tre ordini di benefici, che scaturiscono da questa attività di monitoraggio iniziale:

la possibilità di avere sempre sotto controllo, nei limiti del possibile, il processo di Trattamento, potendo sempre dare risposte adeguate, a seconda dei casi, all'interessato, che eserciti i diritti che la Legge gli riconosce, e al Garante, che disponga controlli e ispezioni, esercitando i poteri che la legge gli assegna;
cogliere il valore aggiunto della legge in termini di organizzazione e di verifica dei flussi informativi interni all'Ente e da questo verso l'esterno;
infine per un maggior coinvolgimento di tutta la struttura, al fine di dare consapevolezza e a far nascere e consolidare una cultura del rispetto della riservatezza degli interessati e quindi a perseguire un miglioramento dei rapporti con la propria cittadinanza e con quanti verranno in contatto con l'Ente.

4) CRITERI DI NOMINA DEI RESPONSABILI DEL TRATTAMENTO E INDIVIDUAZIONE DEGLI INCARICATI

4.1. SCOPO

La presente sezione assolve all'imprescindibile fine di individuare le figure che siano di reale e proficuo supporto all'attività del Titolare del trattamento dei dati personali.
Quanto in appresso muove dall'esigenza di adempiere realmente a quanto previsto dal Testo Unico in Materia di Privacy (D. Lgs 196/03) ed in particolare per fare rispecchiare la situazione reale e fattuale con quella giuridico-normativa e, quindi, con l'assunzione della qualifica di Responsabile del Trattamento da parte di soggetti non solo in possesso delle caratteristiche di competenza, affidabilità e sicurezza ma anche e soprattutto sulla considerazione della loro effettiva e costante supervisione del proprio settore e/o Area Amministrativa dell'Ente, tra queste compresa l'attività di trattamento dei dati personali posta in essere dal Comune di Ragusa
Ad ulteriore corollario degli adempimenti sono stati altresì delineati e individuati per gruppi omogenei gli incaricati per lo svolgimento delle singole operazioni di Trattamento e ciò in base al proprio profilo professionale o di qualifica, al settore e/o servizio in cui svolgono le proprie funzioni amministrative ed in base alle banche dati da essi trattate.

4.2. RIFERIMENTI NORMATIVI

Articolo Norma Descrizione
Art. 29 D.Lgs. 196/03 Responsabile del Trattamento
Art. 30 D.Lgs. 196/03 Incaricati del Trattamento
Allegato B
rif. Artt.da 33 a 36 D.Lgs. 196/03 Accesso ai dati particolari
Art. 4 D.Lgs. 196/03 Trattamento di dati personali

4.3. RESPONSABILITA'

Il T.U. in materia di protezione dei dati personali dispone che il Titolare del Trattamento deve nominare i Responsabili del Trattamento (interni e/o in outsourcing) affidando loro compiti, analiticamente specificati per iscritto, e impartendo istruzioni per il Trattamento dei dati personali.
Il Titolare deve vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni in materia di Trattamento e delle proprie istruzioni.
Il Titolare e, se designati, i Responsabili devono nominare per iscritto i soggetti/incaricati del trattamento al fine di compiere le operazioni di Trattamento: questi devono operare sotto la loro diretta autorità, attenendosi alle istruzioni impartite.
Titolare e Responsabili di Area devono verificare che gli incaricati abbiano accesso ai soli dati particolari (ossia sensibili o giudiziari), per i quali è stato autorizzato l'accesso, in quanto la loro conoscenza sia strettamente necessaria e sufficiente allo svolgimento delle operazioni affidate loro.

Considerata la dimensione e l'organizzazione interna dell'Ente è stato ritenuto necessario procedere alla designazione e nomina dei Responsabili del Trattamento (DPS/ALL 04) che, ai sensi dell'art. 29, sono stati individuati tra soggetti che per esperienza, capacità ed affidabilità, forniscono realmente idonee ed ampie garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Il responsabile nominato non ha il potere di nominare a sua volta altri responsabili ma solo, eventualmente, gli incaricati (interni o esterni) al trattamento.
La nomina dei Responsabili da parte del Titolare è riconducibile al contratto di mandato, disciplinato dagli artt. 1703 e ss c.c. :"Il mandato è il contratto con il quale una parte si obbliga a compiere uno o più atti giuridici per conto dell'altra" e si presume oneroso. Pertanto, qualora il Titolare non intenda riconoscere alcun compenso per gli obblighi assunti, è necessario che ciò sia indicato nell'atto di nomina.
In particolare i responsabili non possono compiere operazioni sui dati che renderebbero illecito il relativo trattamento.
In questo caso risponderebbe giuridicamente il Titolare del trattamento (Amministrazione Comunale), salvo l'eventuale regresso, in presenza delle condizioni di fatto e di diritto, nei confronti dei propri dipendenti.
Nella specificazione dei compiti assegnati ai Responsabili il Titolare ossia l'Ente, rappresentato dal Sindaco prevede che gli stessi devono procedere all'adozione delle misure minime di sicurezza e alla valutazione delle misure idonee da proporre all'organo competente, il quale dovrà procedere alla loro adozione. Inoltre sempre ai Responsabili sono assegnati compiti di verifica dei profili qualitativi e quantitativi dei dati oggetto di Trattamento e di controllo del processo di Trattamento, con obbligo di riferire in sede di conferenza del Gruppo Privacy o al Sindaco pro tempore.
Inoltre i Responsabili devono presentare una relazione periodica al Gruppo Privacy sull'andamento delle attività di Trattamento in seno all'Ente.
In base a quanto sopra evidenziato potranno essere nominati Responsabili del Trattamento il Dirigente/Responsabile pro tempore di Area e/o Settore in cui l'Ente è ripartito.
La scelta di procedere alla nomina con riferimento alla struttura e non alla persona fisica è pienamente compatibile con la definizione di Responsabile del Trattamento, fornita dall''art. 29 del D. Lgs 196/03: può pertanto essere indifferentemente nominata una persona fisica, o l'ufficio della persona che si intende nominare responsabile.
Inoltre nominare l'organismo (l'ufficio), in luogo di una persona fisica, comporta due ordini di vantaggi:
Consente una gestione cd. dinamica: la nomina dei Responsabili come detto è facoltativa.
Tuttavia qualora si decida di procedere in tal senso (e non può essere diversamente, in una struttura come quella di un Comune) occorre indicare tale circostanza nelle informative che vengono fornite agli interessati del Trattamento. Nominare quindi una persona fisica può comportare che in caso di turn over o di revoca di incarichi si debbano rinnovare i due adempimenti considerati. Quindi la scelta di codesto Comune è ispirata alla economicità degli adempimenti e alla flessibilità organizzativa;
il soggetto che rappresenta la struttura nominata Responsabile dei dati personali trattati nel proprio Settore è sempre un dirigente, quindi persona particolarmente qualificata, rispettandosi così il disposto dell'articolo 29 del D.Lgs.196/03.
In caso di mancanza dei suddetti incaricati la nomina, in qualità di Responsabile, può riguardare anche altri soggetti; senza dubbio può essere nominato il Responsabile del procedimento (ai sensi della legge 241/90 e L.R. 30 aprile 1991 n. 10) ovvero il Responsabile dei sistemi informativi automatizzati o infine lo stesso Responsabile unico del procedimento (ai sensi dell'art. 7 della legge 109/94).

4.3.1. Modalità e nomina dei Responsabili

L'art. 28 del Testo Unico n. 196/03 stabilisce che quando il trattamento è effettuato da un Ente pubblico il medesimo assume la qualifica di Titolare del Trattamento in considerazione della sua entità complessiva.
Il Titolare del Trattamento, in persona del Sindaco pro tempore, con propri Decreti provvede a nominare i vari Responsabili di Area, anche in riferimento all'Ordinamento dei servizi e degli uffici del Comune di Ragusa, come previsti dal modello organizzativo.
Allo scopo è stata predisposta idonea documentazione con la specificazione analitica, per iscritto, dei compiti assegnati alle unità Responsabili di cui l'originale deve essere conservato in allegato al Documento Programmatico sulla Sicurezza ed una copia consegnata al Responsabile di Area che contemporaneamente assume, anche la veste di Responsabile del Trattamento dei dati personali
Tale conferimento di Responsabilità deve essere opportunamente firmato per accettazione.

4.3.2. Modalità e designazione degli Incaricati
I Responsabili e il Titolare hanno il potere di incaricare per iscritto determinati soggetti in virtù della loro diretta operatività sui dati. Tale conferimento non ha natura contrattuale ma è un semplice "conferimento di mansioni" e prescrizione di regole e cautele. La nomina dell'incaricato pertanto non comporta alcun onere per il titolare.
Mentre il Responsabile è una figura facoltativa, l'individuazione degli incaricati è obbligatoria, al fine di poter procedere al Trattamento dei dati personali: se così non fosse gli stessi dipendenti dell'Ente non potrebbero aver accesso ai dati personali, né compiere operazioni di Trattamento, se non nel rispetto delle disposizioni, che regolamentano le comunicazioni di dati. Così l'Ente deve provvedere a incaricare tutti i suoi dipendenti per iscritto, impartendo loro istruzioni formali per lo svolgimento delle operazioni di Trattamento.
Occorre però fare due considerazioni, prima dell'individuazione degli incaricati:
la prima riguarda la circostanza che incaricati del Trattamento possono essere solo persone fisiche proprio per il fatto che l'incaricato è colui che svolge materialmente le operazioni di Trattamento;
la seconda considerazione riguarda la possibilità o meno di procedere all'individuazione di incaricati, operanti all'esterno dell'Ente: la circostanza non è esclusa dalla legge, che fa riferimento al fatto che gli incaricati devono operare sotto la diretta autorità del Titolare o del Responsabile. Operare sotto la diretta autorità non comporta che ci debba essere necessariamente un rapporto di lavoro dipendente.
Quindi l'Ente, tutte le volte che decide di dare all'esterno la gestione di un servizio, qualora ciò comporti un trasferimento di dati personali, al fine del Trattamento in suo nome e per suo conto, che sia strettamente necessario al corretto svolgimento dell'incarico affidato, dovrebbe:
nominare la società, associazione, cooperativa Responsabile del Trattamento, ai sensi dell'art. 29 D.Lgs.196/03: è da escludersi la individuazione come incaricato del Trattamento di un Ente o associazione, in quanto questi, per lo svolgimento delle singole operazioni, devono preporre persone fisiche, opportunamente istruite (la legge però non consente ad un incaricato di nominare a sua volta degli incaricati);
nominare una persona fisica esterna indifferentemente Responsabile del Trattamento o incaricato: la scelta per l'una o l'altra figura dipende essenzialmente dal maggiore o minore grado di autonomia, che si vuole concedere nello svolgimento delle attività di Trattamento.
E' bene tenere presente, comunque, che la legge non consente ad un incaricato di nominare a sua volta degli incaricati e che per le nomine degli incaricati non vi è nessun obbligo di trasparenza (es. nell'informativa) o diffusione.
La nomina degli incaricati/dipendenti del Comune di Ragusa Almo è avvenuta secondo i canoni previsti dalla legge ed è stata seguita da appositi incontri per la formazione del personale anche a titolo di misura minima di sicurezza imposta dal punto 19.6 del disciplinare

tecnico in materia di misure minime di sicurezza di cui al D.Lgs. 196/2003 ed in definitiva, per favorire la consapevolezza dei soggetti, cercando di renderli edotti sugli obblighi loro assegnati nonché per prevenire eventi dannosi, responsabilizzare i medesimi soggetti che conoscono le azioni e i comportamenti da adottare affinché pongano in essere le precauzioni e le cautele necessarie per un legittimo Trattamento dei dati personali.
Questo sull'assunto che maggiore è il numero di soggetti che hanno accesso ai dati, maggiori sono i rischi di identificazione dell'interessato e quindi le violazioni potenziali della riservatezza del medesimo.
L'accesso alle diverse tipologie di dati è consentito ai soli incaricati del Trattamento, preposti caso per caso alle specifiche fasi dell'attività amministrativa, secondo il principio della pertinenza dei dati di volta in volta trattati. Questa disposizione prevede che non solo si debba procedere necessariamente alla individuazione degli incaricati, ma che questa nomina avvenga differenziando il profilo di ognuno nell'ambito delle finalità proprie dell'Ente. In applicazione di tale principio di ordine generale ci sono incaricati che perseguono direttamente gli specifici fini del settore di appartenenza; si pensi ad esempio agli impiegati del Servizio amministrativo – Ufficio demografico - ai quali soli compete conoscere tutti i dati riguardanti lo stato civile, le anagrafi ecc... ed ai quali deve essere precluso il Trattamento di dati propri degli altri Servizi dell'Ente. Per quanto detto, per determinate materie e/o per i dati sensibili rimane comunque salva la preclusione a determinati trattamenti di dati personali ad incaricati appartenenti al medesimo settore.
L'autorizzazione deve essere comunque limitata ai soli dati, la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di Trattamento.
Le autorizzazioni all'accesso sono rilasciate e revocate dal Titolare e/o dai Responsabili che periodicamente, e comunque almeno una volta l'anno devono verificare gli incarichi afferenti i dati personali in termini sia di legittimità del Trattamento che della sussistenza delle cautele poste in essere per la conservazione dei medesimi dati.
L'autorizzazione deve essere comunque limitata ai soli dati, la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di Trattamento.
Alla luce delle disposizioni richiamate, si è proceduto alla individuazione degli incaricati in base alle banche dati da essi trattate e in base al servizio o ufficio amministrativo di appartenenza, come riportato dall'Ordinamento dei Servizi e degli Uffici rispetto alla dotazione organica dell'Ente stesso.
L'assegnazione della loro nomina avviene secondo le modalità di nomina individuale, in relazione alle loro funzioni ed in base alle banche dati da essi trattati.
La nomina degli Incaricati avverrà a cura dei Responsabili del Trattamento, ognuno con riferimento al proprio settore/area di competenza, utilizzando la modulistica in allegato al Documento Programmatico sulla Sicurezza, ed in particolare ai seguenti allegati:
DPS/ALL 01.01 – 01.02 – 01.03 – 01.04 "Elenco Incaricati", che costituiscono l'elenco completo ed aggiornato del Personale dipendente dell'Ente o Incaricati del Trattamento;
DPS/ALL 05 " Modulo Nomina Incaricati del Trattamento ".
Per quanto riguarda gli Incaricati esterni si farà riferimento al modello atto di nomina
DPS/ALL 08 applicando la seguente procedura:
inserimento di una clausola nel contratto o nella convenzione o nella determinazione di incarico, stipulata fra l'Ente e l'Incaricato, avente ad oggetto la nomina, con rinvio alle istruzioni, in allegato, costituenti parte integrante del contratto stesso;
definizione del profilo del soggetto preposto al Trattamento;
personalizzazione della lettera di incarico e delle istruzioni;
consegna in duplice copia, una delle quali deve essere restituita, opportunamente firmata per presa visione;

la non accettazione dell'incarico comporta l'impossibilità di dar corso all'esecuzione delle prestazioni dedotte, con la conseguenza della mancata conclusione del contratto stesso o della risoluzione del rapporto in corso di esecuzione.

In conclusione ogni soggetto incaricato deve essere consegnata una copia della lettera e/o-determinazione di incarico, l'originale della quale deve essere sottoscritta e conservata in allegato al Documento Programmatico sulla Sicurezza.

5) ADEMPIMENTI A RILEVANZA INTERNA ED ESTERNA MISURE MINIME DI SICUREZZA

5.1. SCOPO

Scopo della presente sezione è descrivere gli adempimenti necessari cd. a rilevanza interna ed esterna e le azioni che il Comune di Ragusa pone in essere per il trattamento dei dati personali, ed in particolare:
il controllo del processo di Trattamento;
le modalità utilizzate per la predisposizione delle informative agli interessati;
l'adozione di procedure per favorire l'esercizio dei diritti da parte dell'interessato.

5.2. RIFERIMENTI NORMATIVI

Articolo	Norma	Descrizione
Art. 11	D.Lgs.196/03	Modalità di raccolta e requisiti dei dati personali
Art. 7	D.Lgs.196/03	Diritti dell'interessato
Art. 13	D.Lgs.196/03	Informativa
Artt. 20/22/26/62/95/107	D.Lgs.196/03	Dati sensibili
Art. 15	D.Lgs.196/03	Danni cagionati per effetto del Trattamento di dati personali
Art. 167	D.Lgs.196/03	Trattamento illecito di dati personali
Art. 170	D.Lgs.196/03	Inosservanza dei provvedimenti del Garante

5.3. IL CONTROLLO SUI DATI TRATTATI

In particolare l'art. 11 del D.Lgs.196/03 prevede che i dati personali oggetto di Trattamento devono essere: trattati in modo lecito e secondo correttezza: ossia in modo conforme rispetto alle norme giuridiche e alle regole del mestiere informatico. Ecco spiegata la ragione per cui l'Ente ha ritenuto fondamentale, in via preliminare, procedere al monitoraggio del processo di Trattamento in modo da avere il quadro di quanto viene fatto all'interno dell'Ente. In particolare la liceità consiste nella conformità sia alle norme di legge sulla protezione dei dati personali, sia alle altre norme specifiche di settore rilevanti, raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di Trattamento in termini compatibili con tali scopi: la finalità costituisce l'elemento cardine del Trattamento, in tutti quei settori dell'Ente che hanno finalità omogenee o fortemente correlate fra di loro. La finalità non può essere determinata per relationem, o con una tale genericità, che permetta un uso plurimo e imprevedibile dei dati: occorre sempre informare l'interessato degli scopi del Trattamento.
A ben vedere questa è una forma di esplicitazione e di trasparenza anche dell'azione amministrativa dell'Ente; conservati in una forma che consenta l'identificazione

dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
Anche in questo caso è compito del Responsabile procedere ai controlli. (è necessario prestare attenzione su un punto, ossia che, decorso il periodo di tempo necessario al raggiungimento delle finalità di Trattamento, residuano a carico dell'Amministrazione Comunale sia obblighi di documentazione della propria attività amministrativa che ragioni archivistiche per finalità storiche regolamentate dal d.lgs 281/99).
Tra gli obblighi previsti dalla legge vi rientra, anche, quella avente ad oggetto la necessità di effettuare un costante controllo sui dati in ordine alla finalità dei trattamenti posti in essere compatibilmente all'osservanza delle seguenti caratteristiche intrinseche che debbono essere possedute dai dati raccolti:
esattezza: il dato deve riprodurre con esattezza la fonte, che, nel caso di dati sensibili e qualora non sia stata specificamente indicata, si intende rilevata direttamente presso l'interessato;
aggiornamento: obbligo del titolare è quello di aggiornare il dato in relazione a cambiamenti di sostanza e significato proprio sotteso al dato. Per effetto di tale procedura quanto raffigurato in modo statico diverrà oggetto di cambiamento e, per l'effetto, manifestazione dell'esattezza e dell'adeguamento al dato originale. Tale obbligo dovrà essere reso attivo ogni qualvolta l'interessato comunicherà cambiamenti del dato stesso.
pertinenza: trattasi di un elemento fondamentale per la gestione soprattutto degli output. Per tale requisito a fronte di una richiesta di comunicazione occorrerà verificare preliminarmente se il trattamento del dato è giustificato da una previsione normativa (ossia da una legge o da un regolamento) o se l'interessato ha rilasciato il proprio consenso per i casi di trattamento di dati sensibili.
non eccedenza: tale requisito fa riferimento ad un profilo quantitativo. Anche per questo profilo valgono le considerazioni espresse alla lettera precedente con riferimento alla gestione delle operazioni di output;
completezza: attiene sia alla finalità della banca dati, sia ai dati stessi memorizzati.

5.3.1. Le modalità utilizzate per la predisposizione delle informative agli interessati (art. 13 D.Lgs.196/03)
Le informative consistono in documenti esplicativi del trattamento dei dati personali da consegnare alla persona che affida i suoi dati personali all'ente. E' facoltà dei Responsabili del Trattamento adattare la modulistica alle esigenze dell'ente e spetterà poi al Sindaco, in qualità di rappresentante dell'Ente, Titolare del Trattamento, la loro approvazione.
Le informative possono essere fornite agli interessati anche dagli incaricati del Trattamento, con libertà di forme decise dai Responsabili di Area.
Premesso che il Trattamento di dati personali effettuato da codesto Ente non è condizionato dal previo consenso dell'interessato e premesso inoltre, che nonostante il Testo Unico in materia di protezione dei dati personali abbia previsto la possibilità di fornire una informativa anche orale, il Comune di Ragusa ha ritenuto comunque necessario fornire sempre un'informativa scritta all'interessato al fine di permettere il raggiungimento ed il soddisfacimento degli scopi previsti nell'art.13 del D.Lgs.196/03 e garantire ai propri cittadini un reale, efficace e trasparente controllo del Trattamento dei dati personali che li riguardano.
Per completezza si ricorda che :
l'informativa ha lo scopo di consentire all'interessato di conoscere l'identità di chi tratta dati personali che lo riguardano e per quali finalità e modalità ed è essenziale proprio per permettere di esercitare un controllo in ordine ai diritti riconosciuti dalla legge e circa il corretto utilizzo dei propri dati personali;
l'art. 13 indica una serie di informazioni che devono essere necessariamente rese tramite l'informativa e sotto la diretta responsabilità del Titolare del Trattamento dei dati personali.

Quest'obbligo risponde ad una precisa ratio dell'adempimento, che come tale, è finalizzato a rendere edotto l'interessato sull'identità dei soggetti istituzionalmente previsti ed appositamente preposti al Trattamento dei dati che lo riguardano e su tutte le circostanze del processo stesso.
Le informazioni da fornire riguardano:
le finalità e le modalità del Trattamento;
la natura obbligatoria o facoltativa del conferimento dei dati;
le conseguenze di un eventuale rifiuto di rispondere;
i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
i diritti di cui all'articolo 7;
il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del Titolare e, se designato, del Responsabile.
A ben vedere sono riportati diversi elementi, che sono stati oggetto di monitoraggio attraverso l'uso della scheda di processo il fine infatti è proprio quello di raccogliere una serie di informazioni per ogni singola unità di Trattamento complessa e di base al fine di predisporre i moduli di informativa (VET/ALL 05.01).
Al fine della armonizzazione degli schemi di informativa, e che possono essere adattati, a seconda delle esigenze, dai Responsabili del Trattamento, si precisa che tali schemi debbono osservare sempre la seguente struttura:
un cappello, con una formula comune, in cui viene presentata la legge e le procedure applicate dall'Ente in materia di Trattamento di dati personali;
un corpo centrale, costituente la parte dinamica, che ogni Responsabile può adattare alle proprie esigenze tenendo fermo le condizioni di coordinamento sopra espresse. In questa sezione sono riportate le cd. informazioni opportune e quelle eventuali;
una coda, in cui sono riportati gli elementi ritenuti necessari (indicazione del Titolare e richiamo ai diritti dell'interessato).
Infine per quanto riguarda le modalità di diffusione delle informative si può provvedere nel seguente modo:
rapporti di front-office: predisposizione di manifesti affissi agli sportelli a cura dei responsabili e per ciascuna sede di operatività del Comune;
servizi a domanda individuale: informativa in calce ai moduli, che devono essere eventualmente compilati, in particolare quelli per le autocertificazioni, come previsto dall'art. 48 del d.P.R. 445/2000;
procedure concorsuali (selezione personale, gare di appalto): inserimento della formula di informativa nei relativi bandi;
in via residuale pubblicazione delle informative e della politica in materia di privacy sul sito web del Comune.
Per concludere l'art. 13 comma 4 dispone che quando i dati personali non sono raccolti presso l'interessato, l'informativa è data al medesimo interessato all'atto della registrazione dei dati o, qualora sia prevista la loro comunicazione, non oltre la prima comunicazione.
Questa disposizione non si applica quando:
i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento e dalla normativa comunitaria;
i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui all legge 7 dicembre 2000, n. 397 o, comunque per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
l'informativa comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

5.3.2. Il consenso per il trattamento dei dati sensibili e/o giudiziari

Di norma, come si è avuto modo di evidenziare in precedenza, i soggetti pubblici possono procedere al Trattamento dei dati personali senza dover richiedere il consenso degli interessati.

La legge infatti prevede in generale il principio di finalità istituzionale, con regole particolari a seconda della natura dei dati trattati.

Qualora oggetto del Trattamento siano i dati comuni, trova applicazione l'art. 18 del D.Lgs.196/03, che prevede che il Trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge o dai regolamenti (questa regola è strettamente connessa al principio di legalità dell'azione amministrativa).

Più complessa ed articolata risulta la normativa di principio riferita ai dati sensibili e giudiziari (artt. 20 e 21 D.Lgs.196/03), il loro trattamento da parte di enti pubblici è consentito solo se è previsto da espressa disposizione di legge o provvedimento del Garante che specificano i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Il legislatore ha previsto una triplice garanzia al fine di tutelare gli interessati:

Occorre sempre una norma di rango legislativo ed espressa;

La norma deve esplicitare il rilevante interesse pubblico;

La norma deve indicare analiticamente operazioni e trattamenti eseguibili.

5.3.3. L'adozione di procedure per favorire l'esercizio dei diritti da parte dell'interessato

Per favorire l'esercizio dei diritti previsti dall'art. 7-10 D.Lgs. 196/03 l'Ente adotterà delle misure occorrenti per facilitarne l'esercizio. A tal proposito si adotterà una apposita procedura (VET/ALL 05.02), disciplinante le modalità per rispondere alle richieste di accesso degli interessati che potranno essere effettuate mediante un modello prestampato (VET/ALL 05.03), da richiedere presso gli uffici

5.4. ALLEGATI

VET/ALL 05.01 Modelli per le informative agli interessati

VET/ALL 05.02 Procedura per la gestione delle richieste degli interessati

VET/ALL 05.03 Modulo per l'esercizio dei diritti da parte dell'interessato

6) MISURE MINIME DI SICUREZZA PER IL TRATTAMENTO

6.1. SCOPO

Il D. Lgs. 196/03 impone, tra i diversi obblighi, che il Titolare adotti un insieme di misure di sicurezza a tutela dei dati personali oggetto del trattamento volte ad assicurare un livello di protezione adeguato al tipo di trattamento effettuato.
Pertanto i dati personali oggetto del trattamento devono essere custoditi e controllati in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento così da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Per tale motivo il legislatore ha previsto, agli artt. 31-36 del D. Lgs 196/03, una serie di norme relative alle c.d. misure minime che devono essere adottate per qualunque tipo di trattamento. Ad esse devono aggiungersi le misure idonee, più intense, specifiche per quei trattamenti che presentano rischi particolari o che sono relativi a dati sensibili.
Inoltre l'allegato B al D. Lgs 196/03 (Disciplinare Tecnico) elenca tutte le prescrizione di legge per il caso in cui il trattamento sia effettuato con strumenti elettronici e non. Per il primo caso, qualora l'azienda tratti dati sensibili o particolari e qualora ritenga di non poter adempiere con le sue sole risorse all'adozione delle misure necessarie, potrà incaricare un esperto informatico il quale dovrà provvedere a certificare la conformità delle misure adottate alle prescrizioni di legge.
Infine ulteriori prescrizioni sono state rese note dal Garante tramite provvedimenti pubblicati nel sito istituzionale www.garanteprivacy.it.
Sono riportati qui di seguito sia gli articoli dal 31 al 36 del Decreto, sia le norme del disciplinare tecnico al fine di un più agevole controllo e costante monitoraggio delle misure di sicurezza adottate all'interno dell'azienda.
Si è ritenuto di omettere brevi note di commento in quanto i singoli punti di tali disposizioni sono già stati ampiamente illustrati in seno ai corsi di formazione tenutisi presso i locali dell'azienda e anche in tutto il corpo del presente documento esplicativo del trattamento.
Tuttavia in calce alla trascrizione delle norme è stato approntato un elenco di consigli pratici, utile supporto alla concreta applicazione del decreto legislativo.
L'omissione delle misure minime di sicurezza configura l'ipotesi di reato prevista all'art. 169 del D. Lgs 196/03 la cui sanzione è costituita dall'arresto fino a due anni o con l'ammenda da diecimila a cinquantamila euro.

6.2 GLI ARTICOLI 31-36 D. LGS 196/03

Art. 31. Obblighi di sicurezza
1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 32. Particolari titolari

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

Art. 33. Misure minime

Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36. Adeguamento
Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

6.3. IL DISCIPLINARE TECNICO (ALLEGATO B)

TRATTAMENTI CON STRUMENTI ELETTRONICI

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

SISTEMA DI AUTENTICAZIONE INFORMATICA

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando

preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

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

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

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. 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;
19.5. 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;
19.6. 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 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;
19.7. 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;

19.8 per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. 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.

22. 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.

23. 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.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

MISURE DI TUTELA E GARANZIA

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

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

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

6.4 CONSIGLI PRATICI

Trattamento con strumenti elettronici

- Attribuzione di un codice identificativo per ogni PC: E' indispensabile attribuire a ciascun pc un numero identificativo mediante l'apposizione di un adesivo recante numeri progressivi. Ciò al fine di una migliore identificazione della postazione di lavoro all'interno del Documento Programmatico sulla Sicurezza (DPS)
- Backup dei dati almeno settimanale: La copia dei dati contenuti sui PC e/o sul server deve essere effettuata con cadenza almeno settimanale o più spesso ove se ne ravvisi la necessità. I supporti di memorizzazione più idonei sono i cd rom in quanto i floppy sono soggetti a frequente smagnetizzazione. La copia di backup deve essere custodita in cassaforte, meglio se in un luogo fisicamente lontano da quello ove i dati originali si trovano per evitare che eventi quali l'incendio o l'allagamento possano distruggere entrambe le copie.
- Autenticazione informatica: E' necessario attribuire a ciascun utente dei PC una User ID e una password di accesso sia ai dati contenuti sul PC, sia alla rete informatica.
- Aggiornamento almeno settimanale software antintrusione: I software antintrusione o antivirus possono essere impostati in modo tale da effettuare l'aggiornamento in maniera automatica, ogni volta che la software house invia agli utenti l'aggiornamento per la protezione dai nuovi virus. Pertanto è opportuno inserire tale modalità di aggiornamento. Ritenuto particolarmente alto il rischio di perdita di dati a causa di intrusioni informatiche, sarebbe opportuno dedicare alcuni PC solo al collegamento ad internet così da escludere il collegamento a quei PC ove i dati risiedono.
- Password: Le password necessarie sono almeno 3: La password da digitare all'accensione del PC, insieme alla User ID (nome utente); La password di accesso alla rete, necessaria per autenticare l'accesso alla rete LAN (rete interna); quella dello screen saver, necessaria al fine di oscurare i dati a video in caso di inattività dell'operatore per almeno 2 minuti. La Password, che deve essere composta da una sequenza priva di significato, preferibilmente alfanumerica, deve essere composta da almeno otto caratteri (se l'elaboratore lo consente) e non deve contenere riferimenti a nomi o date o comunque altre parole facilmente riconducibili all'utente. Es. di password valida: xh67mnhi987.
La Password deve rimanere segreta e comunicata solo al soggetto nominato custode delle password. La parola chiave deve essere inserita in una busta chiusa, sigillata e controfirmata sui lembi, busta che l'incaricato del trattamento dovrà consegnare al preposto che ne curerà la conservazione. Modificare la parola chiave almeno ogni sei mesi per il trattamento di dati comuni; ogni tre mesi in caso di trattamento di dati sensibili e giudiziari.
- Utilizzazione di un sistema di autorizzazione: Ciascun incaricato deve poter avere accesso solo ai dati strettamente indispensabili all'espletamento dell'attività lavorativa che gli compete. Pertanto in caso di PC condiviso fra più utenti o in presenza di rete LAN, è necessario che ciascun utente sia autorizzato ad accedere solo ai dati necessari, escludendo la possibilità di accessi non autorizzati ad aree o cartelle presenti sul server o su altri client di pertinenza di altri incaricati.
- Adozione di antivirus, firewall, router, ecc.: A tal fine è necessario acquistare software antivirus originali e far installare da tecnici informatici competenti in materia di privacy firewall o router idonei alla natura dei dati trattati.
- Fax: Evitare di posizionare il fax in un luogo accessibile a l pubblico.

- Supporti informatici: Particolari cautele sono prescritte per i supporti di memorizzazione informatica. Se è stata fatta copia dei dati sensibili su supporti informatici (floppy, CD rom ecc.) gli stessi non possono essere usati da persone diverse da quella che ha eseguito la copia dei dati se gli stessi non sono stati cancellati con l'ausilio di particolari programmi software. Ciò perché i dati non vengono cancellati in maniera definitiva dai supporti in quanto è sempre possibile ripristinarli tramite appositi programmi. Qualora i dati contengano dati comuni è sufficiente la cancellazione dei dati "tradizionale" prima dell'uso da parte di persona diversa da quella che li ha memorizzati. La distruzione di tali supporti deve avvenire mediante rottura degli stessi prima di cestinarli.
- Rapporti Log file: I file di Log sono registri informatici che memorizzano le operazioni eseguite dagli utenti. Possono essere paragonati ad un diario di bordo. I log file sono indispensabili, oltre che per ricostruire gli accessi degli incaricati al PC (accessi anche esterni, da parte di soggetti non autorizzati come hacker), anche per lasciare traccia delle copie di backup ecc.. E' pertanto necessario che i PC siano impostati così da essere presenti i registri dei log opportuni per le esigenze privacy.
- Gruppo di continuità: Evita che sbalzi di tensione elettrica possano danneggiare il PC e i dati in esso contenuti.
- Continuità alimentazione elettrica: Evitano che l'improvvisa assenza di corrente elettrica provochi la perdita dei dati non ancora salvati.
- Contratti di assistenza Hardware e Software PC: per un maggior controllo degli strumenti informatici, al fine di ridurre i rischi propri dei sistemi informatici, è opportuno che l'Ente preveda di stipulare contratti di assistenza con un azienda specializzata o tecnici informatici che certifichi la conformità della rete informatica alle prescrizioni del decreto Legislativo sulla privacy. Ciò anche al fine di nominare lo stesso amministratore di sistema e di concordare con lo stesso la procedura per il ripristino dei dati in caso di perdita accidentale dei dati. Di tale procedura deve farsi menzione del DPS.
- Verifica periodica funzionalità apparecchiature: Per la migliore tutela dei dati è necessaria la periodica verifica della loro funzionalità.
- Sistemi di criptazione dei dati sensibili: Il D. Lgs 196/03 prescrive per gli enti pubblici la criptazione per la conservazione o per la trasmissione telematica dai dati sensibili o la separazione fra i dati sensibili e quelli comuni. Nel primo caso è necessario dotarsi di appositi software. Nel secondo è necessario stabilire delle procedure per le quali i dati sensibili vengono conservati, custoditi e archiviati con modalità separata e distinta dai dati comuni. A titolo meramente informativo sono riportate di seguito le regole cui attenersi per la crittografia dei dati: Quanto alla crittografia, è necessario definire il profilo di autorizzazione dell'incaricato in relazione ai dati sensibili cui ha accesso e che possieda e sia dotato di una chiave di cifratura o decifratura dei dati stessi. L'utilizzo e la predisposizione di una chiave crittografica per il trattamento dei dati sensibili introducendo un elevato livello di protezione per il loro trattamento garantisce in definitiva quanto sotteso dal disposto normativo. Per quanto sopra l'incaricato del trattamento dei dati sensibili può essere: autorizzato a leggere i dati (per il qual caso è sufficiente che conosca la chiave di decifratura); autorizzato a creare e/o modificare i dati (per il qual caso deve conoscere la chiave di cifratura dei dati crittografati). Effettuata questa disamina il Titolare del Trattamento dei dati personali nel caso in cui vi sia questo trattamento di dati dovrà predisporre la seguente procedura per la gestione delle chiavi che si aggiunge a quella di autenticazione informatica già analizzata.
In particolare si è predisposto e deve osservarsi quanto segue:
La chiave deve essere generata mediante procedure sicure di creazione; deve essere custodita da soggetti con comprovata conoscenza tecnica e di indubbia affidabilità;
deve essere concessa dal Responsabile del Trattamento solo agli incaricati del Trattamento il cui profilo di autorizzazione comprende l'accesso ai dati crittografati.

Con queste tecniche i dati sensibili in questione possono essere archiviati nel sistema informatico centrale con estrema sicurezza perché l'accesso alla consultazione e/o alla modificazione dei dati sensibili sarà sempre condizionato dal rispetto della procedura sopraesposta ed in definitiva dei seguenti criteri in base ai quali:
L'incaricato deve essere precisamente individuato ed autenticato;
L'incaricato può trattare i dati sensibili solo con un appropriato profilo di autorizzazione;
L'incaricato deve essere in possesso della chiave di lettura o cifratura.
Per quanto detto e per le menzionate procedure gestionali dei dati sensibili deve evidenziarsi in definitiva che i dati sensibili debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato unicamente in base al proprio profilo di autorizzazione.
- Backup delle e-mail: Le e-mail inviate devono sempre essere conservate in copia e deve sempre essere richiesta la conferma di ricevimento al destinatario.
- Corsi di alfabetizzazione informatica incaricati del trattamento: E' frequente che per la scarsa competenza informatica degli addetti al trattamento si possano accidentalmente cancellare dei dati o che gli stessi possano essere messi a rischio di "intrusioni informatiche esterne". Un preparazione almeno sufficiente degli incaricati è la misura di sicurezza più importante prescritta dalla legge.
- Software vietato: E' vietato utilizzare software non ufficialmente rilasciato dall'azienda titolare del trattamento e preventivamente testato nella sua integrità e comunque strettamente indispensabile all'espletamento dell'attività lavorativa.. La sicurezza dei dati può essere messa a repentaglio anche da software apparentemente innocui ma che potrebbero creare conflitti interni o aprire l'ingresso ad intrusioni informatiche.

TRATTAMENTI CARTACEI
- Apparecchiature per la distruzione dei documenti cartacei: Esistono dei cestini elettrici per la distruzione dei documenti cartacei. Il costo è basso e assicurano la distruzione totale dei documenti non più utili.
- Archivi: Devono essere dotati, come tutti i locali in cui i dati personali si trovano, di sistemi antincendio, di allarme, e di autenticazione degli accessi.
- Trasferimento di dati all'interno dell'Ente: Per il trasferimento di dati all'interno dell'Ente è necessario far viaggiare i documenti in busta chiusa.
- Aggiornamento dell'ambito di trattamento di ciascun incaricato: Le mansioni di ciascun incaricato possono mutare nel tempo. Aggiornare sempre il sistema di autorizzazione agli accessi in relazione alle mansioni attualmente svolte. Si fa presente che tali modifiche devono essere riportate anche nel DPS.
- Controllo fotocopie (con chiave o password e registrazione numero copie): Evitare di affidare il servizio fotocopiatura dei documenti a persone diverse dall'incaricato autorizzato a trattare i dati contenuti nel documento da fotocopiare. Una macchina fotocopiatrice disponibile a chiunque consente la facile riproduzione dei documenti a persone non autorizzate al trattamento.

SICUREZZA LOGISTICA
- Integrità delle aree e dei locali: I locali devono essere tutelati da intrusioni esterne. Pertanto sarebbe opportuno acquistare vetri antisfondamento, portoncini d'ingresso blindati, installare allarmi e adottare tutte le misure di sicurezza previste dalle vigenti norme ISO.
- Chiusura a chiave degli uffici: Le porte di ingresso degli uffici devono essere chiuse a chiave alla fine dell'orario di lavoro e ogni volta che gli occupanti della stanza dovessero temporaneamente allontanarsi.
- Chiusura a chiave di armadi, cassetti e classificatori: Misura di sicurezza particolarmente importante. Tutte le pratiche, gli elenchi nominativi, o comunque tutto ciò che contenga dati

personali deve essere tenuto sotto chiave. Ciò significa che nulla deve essere lasciato incustodito o comunque visibile sulla scrivania soprattutto se trattasi di ufficio aperto al pubblico.

- Custodia in armadi blindati o ignifughi: Si intende prevenire l'accesso abusivo ai dati sensibili e la distruzione degli stessi a causa di incendio presso i locali ove i dati sono custoditi.

- Casseforti: Qualora le dimensioni della cassaforte lo consentano ed in assenza di rimedi alternativi, i dati sensibili devono essere custoditi in cassaforte. La stessa prescrizione è valida per i supporti di memorizzazione contenenti le copie di backup.

- Distanze di cortesia: Al fine di evitare illecite comunicazioni di dati agli utenti, è necessario predisporre distanze di cortesia agli sportelli di accesso al pubblico.

Documento informativo ai sensi e per gli effetti di cui all'articolo 13, D. Lgs. 30 giugno 2003 n. 196

Nel predisporre la modulistica per adempiere a quanto previsto dall'art. 13 D.Lgs.196/03 si è pensato di prevedere una struttura standard comprendente:
un cappello: in cui compare la presentazione dell'Ente e della politica sulla privacy;
un corpo centrale: la cd. parte dinamica, in cui sono inseriti gli elementi che cambiano a seconda della tipologia di trattamento;
una coda, in cui ci sono i riferimenti all'identità del titolare, dei responsabili e ai diritti previsti dall'art. 7 in capo all'interessato.

Decreto Legislativo n.196/2003, Art. 7 - Diritto di accesso ai dati personali ed altri diritti
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.
I modelli elencati nelle pagine seguenti possono essere usati dal Comune di Ragusa come direttive generali alle quali uniformare i trattamenti effettuati, adattandoli di volta in volta alle esigenze del caso.

Modello n. 1 – informativa ai Dipendenti ai sensi e per gli effetti di cui all'articolo 13, D. Lgs. 30 giugno 2003 n. 196

Informativa ai sensi dell'art. 13 del D.Lgs. 196/2003 il COMUNE DI RAGUSA TITOLARE DEL TRATTAMENTO, La informa che per quanto riguarda la tutela della privacy ha provveduto ad adottare gli adempimenti necessari stabiliti sia nel Vademecum Esplicativo del Trattamento e sia nel Documento Programmatico sulla Sicurezza, ove sono anche riportate, le istruzioni impartite ai propri dipendenti, al fine di migliorare l'erogazione dei propri servizi e di garantire la tutela della riservatezza dei propri dipendenti.
Tali documenti sono in visione presso i singoli Dirigenti di Settore.
I suoi dati personali sono trattati per finalità strettamente correlate alla gestione del rapporto di lavoro con il Comune di Ragusa.
In particolare gli scopi specifici riguardano:
il trattamento giuridico ed economico del personale;
l'adempimento di obblighi fiscali, previdenziali e assistenziali;
la gestione del personale, la valutazione da parte dei dirigenti e le eventuali procedure selettive per la progressione orizzontale e verticale;
adempimenti connessi all'eventuale iscrizione ad un sindacato e all'esercizio dei diritti sindacali;
l'applicazione della normativa specifica in materia di igiene e sicurezza nei luoghi di lavoro (in particolare obblighi di sorveglianza medica, ai sensi del d.lgs. 626/94 e successive modificazioni, d. lgs. 81/2008);
gli adempimenti connessi alla stipulazione di forme assicurative obbligatorie e volontarie;
la difesa di un interesse in sede amministrativa e giudiziaria;
l'eventuale attività disciplinare.
I dati sono raccolti all'atto dell'assunzione e nel corso dell'esecuzione del rapporto di lavoro e possono riguardare anche il coniuge, i figli e altri familiari o congiunti, in relazione al pagamento di indennità speciali, assegni familiari e altri contributi speciali normativamente previsti.
La informiamo che possono essere trattati anche dati di natura sensibile, come ad esempio dati idonei a rivelare lo stato di salute, l'adesione ad un sindacato, adesione a partiti politici, convinzioni religiose, (devoluzione 8 per mille), origini razziali od etniche, ecc...
I dati personali sono raccolti e trattati con mezzi automatizzati e in modo cartaceo, ad opera di soggetti di ciò appositamente incaricati secondo una logica strettamente connessa alle finalità descritte.
I dati sono comunicati solo ove vi sia una previsione di legge o di regolamento, o comunque, nel caso di soggetti pubblici, sia necessario per l'esercizio di una finalità istituzionale.
In particolare le categorie di soggetti destinatari sono:
1) Enti assistenziali e previdenziali;
2) Banche e Istituti bancari;
3) Imprese assicurazione;
4) Studi professionali e di consulenza;
5) Organismi sanitari, personale medico e paramedico;
6) Enti territoriali e istituzionali.
Il conferimento dei dati è obbligatorio per la esecuzione degli obblighi nascenti dal contratto di lavoro.
Il conferimento dei dati relativi ai propri familiari è obbligatorio in quanto connesso alla prestazione richiesta, e un eventuale rifiuto può comportare l'impossibilità di percepire quanto spettante.

I dati non sono diffusi, salvo quelli relativi allo stato giuridico o alle vicende lavorative, che siano oggetto di atti deliberativi o di determinazioni, che devono essere pubblicati all'albo pretorio. È comunque esclusa la diffusione dei dati relativi alla salute sia del dipendente, sia dei familiari o prossimi congiunti.

Eventualmente aggiungere: La informiamo altresì che, per finalità di protezione dei dati e degli apparati di elaborazione l'Ente ha provveduto ad installare sistemi di sicurezza, che possono anche comportare un controllo indiretto dell'attività lavorativa: come ad esempio file di log, firewall,... , tenuto conto del rapporto dell'autorità Francese per la protezione dei dati che nel febbraio del 2002 ha affermato che gli archivi delle connessioni (i cosiddetti file di log),che registrano tutte le connessioni o i tentativi di connessione ad un sistema informatico, hanno finalità eminentemente di sicurezza e non di controllo del lavoratore. Il lavoratore deve comunque essere informato dell'esistenza di questo tipo di archivi e della durata di conservazione dei dati, conservazione che l'autorità competente ritiene ragionevole fissare, ancora una volta, in sei mesi. Per l'attuale legislazione Italiana è importante raggiungere accordo ai sensi dell'art. 4 della legge 300/70 (cd. Statuto dei Lavoratori). Si ricorda inoltre che le postazioni di lavoro, nonché connessioni ad Internet, dal proprio elaboratore, sono, per motivi di sicurezza, ai sensi della legge sulla privacy e all'adozione delle misure minime di sicurezza (di tipo informatico), costantemente controllate attraverso registrazioni di log, che sono periodicamente controllate da parte dell'amministratore di sistema, al fine di verificare condotte illecite o comunque in violazione delle istruzioni impartite ad ogni incaricato del trattamento. Infine si rammenta che la posta elettronica può essere utilizzata solo per finalità di ufficio e di lavoro: si deve evitare quindi di inviare o ricevere messaggi di natura personale, non inerenti all'attività svolta.

Lei potrà far valere i propri diritti come espressi dagli artt. 7, 8, 9 e 10 del D. Lgs. 30 giugno 2003 n. 196, presentando istanza ad uno dei Responsabili del Trattamento, richiedendo l'apposito modulo all'URP o all'indirizzo sopra riportato.

Titolare o Responsabile del Trattamento è il COMUNE DI RAGUSA– CORSO ITALIA 72 RAGUSA

Luogo e data

IL Titolare o Responsabile del Trattamento o

Modello n. 2 – Informativa ai cittadini che conferiscono dati per attività e procedimenti sviluppati dal Comune di Ragusa
(art.13 D.Lgs.196/03)

Informiamo i cittadini ai sensi dell'art. 13 del D.Lgs.196/03 che il COMUNE DI RAGUSA per garantire la migliore qualità ed efficienza dei propri servizi, ha la necessità di richiedere dati e informazioni riguardanti la vita privata delle persone. Queste informazioni vengono richieste soltanto nei casi in cui siano indispensabili alla programmazione ed erogazione di servizi pubblici, nonché allo sviluppo dell'attività amministrativa ed esclusivamente nell'interesse degli utenti. Informiamo inoltre i cittadini che per quanto riguarda la tutela della privacy codesto Ente ha adottato gli adempimenti necessari stabiliti dal D.Lgs. 196/03 in "materia di protezione dei dati personali" e come riportati sia nel Vademecum Esplicativo del Trattamento e sia nel Documento Programmatico sulla Sicurezza, ove sono anche definiti, le istruzioni impartite ai propri dipendenti, al fine di migliorare l'offerta dei propri servizi e di garantire la tutela della riservatezza dei propri utenti.

Tali documenti sono in visione presso l'URP o presso i singoli Responsabili di Servizio. I dati anagrafici, fiscali e reddituali, nonché i dati riguardanti fatti, stati e qualità relativi alla persona o a suoi familiari o a soggetto giuridico rappresentato, sono raccolti e protetti in base alla legge, che tutela la privacy dei cittadini (D. Lgs. 30 giugno 2003 n.196), e potranno essere trattati così come di seguito specificato:

finalità strettamente connesse agli adempimenti di obblighi previsti dalla legge, dallo statuto del Comune, dai regolamenti, dalla normativa comunitaria;

finalità strettamente connesse alla gestione dei procedimenti amministrativi avviati d'ufficio o per iniziativa del cittadino;

finalità connesse allo sviluppo di attività rientranti tra i fini istituzionali dell'Ente.

Il conferimento dei dati è obbligatorio per lo sviluppo dei procedimenti amministrativi avviati d'ufficio o su iniziativa del cittadino, il rifiuto di fornire in tutto o in parte dati personali potrà comportare la mancata attivazione o la sospensione dei procedimenti amministrativi per i quali i dati sono stati richiesti come elementi informativi essenziali.

I dati anagrafici, fiscali e reddituali, nonché i dati riguardanti fatti, stati e qualità relativi alla persona o a suoi familiari o a soggetto giuridico rappresentato possono essere comunicati, in base a quanto previsto da leggi e regolamenti a: altre pubbliche amministrazioni;

soggetti privati: per lo sviluppo di servizi pubblici resi agli interessati nella misura strettamente necessaria allo svolgimento del servizio; per la difesa di interessi giuridicamente rilevanti.

L'ambito di diffusione dei dati personali di cui sopra è il territorio nazionale. E' possibile che per esigenze connesse allo sviluppo dei procedimenti amministrativi, i dati siano comunicati a soggetti pubblici e privati nell'ambito dell'Unione Europea o in ambito Extracomunitario: in tal caso il Comune di Ragusa avrà cura di assicurare ogni cautela per il trasferimento dei dati.

Lei potrà far valere i propri diritti come espressi dagli artt. 7, 8, 9 e 10 del D. Lgs. 30 giugno 2003 n. 196, presentando istanza ad uno dei Responsabili del Trattamento, richiedendo l'apposito modulo all'URP o all'indirizzo sopra riportato.

Decreto Legislativo n.196/2003, Art. 7 - Diritto di accesso ai dati personali ed altri diritti

Titolare del Trattamento è il COMUNE DI RAGUSA.

Per potere ottenere informazioni relative al trattamento dei dati personali conferiti presso questa struttura ci si può rivolgere presso i singoli Dirigenti di Settore.

Modello n. 3 – Informativa per utenti servizi socio-assistenziali

In osservanza di quanto previsto dal D. Lgs. 30 giugno 2003 n. 196, siamo a informarLa che per quanto riguarda la tutela dei dati personali il COMUNE DI RAGUSA ha provveduto ad adottare gli adempimenti necessari stabiliti dal D.Lgs. 196/03 in "materia di protezione dei dati personali" al fine di migliorare l'offerta dei propri servizi e di garantire la tutela della riservatezza dei propri utenti.

Tali documenti sono in visione presso l'URP o presso i singoli Responsabili di Servizio.

1) Formula per il riccometro o sanitometro

La informiamo che i dati vengono raccolti ai sensi del d. lgs. 109/98 (cd. redditometro) o del d. lgs. 124/98 (cd. sanitometro), al fine di procedere alla valutazione della ricchezza per verificare il diritto di ricevere gratuitamente o a prezzo agevolato l'erogazione di una data prestazione sociale.

Il trattamento può riguardare dati riferiti anche a terzi (familiari, conviventi).

I dati richiesti devono essere necessariamente forniti per poter usufruire dei servizi richiesti e per consentire la verifica del suo reddito, ai fini del calcolo dell'ISEE.

Un eventuale rifiuto potrà comportare, a seconda dei casi, l'impossibilità di beneficiare dei servizi, delle prestazioni o dei contributi richiesti.

I suoi dati vengono trattati con strumenti automatizzati e non, comunque con logiche strettamente connesse alle finalità per cui vengono raccolti.

Le informazioni raccolte possono essere comunicate ai soggetti erogatori delle prestazioni richieste, nonché ai soggetti pubblici istituzionalmente competenti.

2) Formula per le autocertificazioni

La informiamo che i dati richiesti con la compilazione del modulo di autocertificazione vengono trattati al fine di verificare stati, fatti e qualità ai sensi del d.P.R. 445/2000.

I dati devono essere conferiti necessariamente al fine della dichiarazione sostitutiva di certificazione o per la dichiarazione sostitutiva di atto di notorietà.

I dati vengono raccolti direttamente presso l'interessato, ma possono riguardare anche terzi (ad esempio familiari, conviventi,...).

I dati inoltre vengono trattati con sistemi automatizzati (registrati in database elettronico) e con sistemi cartacei.

I dati possono essere comunicati ai soggetti istituzionalmente preposti all'erogazione delle prestazioni richieste, ovvero ai soggetti competenti allo svolgimento dei controlli istituzionali (ad esempio ASL di appartenenza, regioni, ...).

I dati non vengono diffusi.

3) Formula per i servizi socio-assistenziali

La informiamo che i dati da Lei forniti vengono trattati per finalità amministrativo-contabili e di assistenza sociale.

Ad esempio: ai fini della valutazione della sua situazione economica e per il versamento di contributi di carattere socio assistenziale (assegni per il nucleo familiare e di maternità ai sensi degli artt. 65 e 66 della legge 23 dicembre 1998, n. 448);

per il reddito minimo di inserimento ai sensi del d. lgs. 237/98;

per il contributo economico per l'affitto di abitazioni (legge 431/98 e d.m. 7 giugno 1999);

per l'organizzazione e la fornitura di servizi di assistenza domiciliare a persone portatrici di handicap, anziani, ...;

per la gestione di programmi di cura e recupero di tossicodipendenti.

I dati vengono trattati sia con modalità automatizzate, sia non automatizzate e comunque con logiche strettamente correlate alle finalità di cui sopra.

Il trattamento dei dati può riguardare anche soggetti terzi (ad esempio familiari,convivente,...) per finalità di anamnesi medica e per fini economici (reddito familiare, contributivi assistenziali,...).
Il conferimento dei dati è facoltativo, ma un eventuale rifiuto può comportare l'impossibilità di:
- usufruire dei servizi richiesti;
- beneficiare di contributi e assegni;
- avere agevolazioni di natura economico-assistenziale.

La informiamo che in alcuni casi può essere necessario procedere al trattamento di dati cd. sensibili, in particolare relativi allo stato di salute: salva la possibilità in alcune situazioni di poter usufruire dell'anonimato, così come previsto espressamente dalla legge (ad esempio per i tossicodipendenti), l'Ente titolare del trattamento procedono al trattamento delle informazioni di tale specie nel rispetto dei principi e delle regole stabilite dalla legge sulla privacy, adottando idonee misure di sicurezza descritte nel Documento Programmatico sulla Sicurezza consultabile a richiesta presso l'Ufficio Relazioni con il Pubblico.
I dati possono essere comunicati ai seguenti enti:
comune di residenza; regione; azienda unità sanitaria locale di appartenenza; soggetti gestori di strutture di soggiorno e di assistenza; cooperative sociali; assistenti sociali; personale sanitario; istituti bancari per finalità contabili e per il versamento delle provvidenze richieste; compagnie di assicurazione: in alcuni casi l'ente può procedere ad una denuncia cautelativa, che può comportare la comunicazione dei dati identificativi del soggetto che ha subito un infortunio o una lesione personale.
Sarà quindi onere dell'interessato consegnare alla compagnia assicurativa la propria documentazione sanitaria, al fine di richiedere e ottenere l'eventuale risarcimento.
Alcune informazioni possono essere comunicate a consulenti fiscali e commerciali e a legali di fiducia rispettivamente per finalità contabili e amministrative e per scopi di tutela in sede giudiziale e stragiudiziale.
Infine i dati possono essere trasferiti, per finalità determinate, ad organi di polizia giudiziaria.
I dati non vengono diffusi, se non nella misura in cui sia necessario per finalità di pubblicità e trasparenza dell'attività amministrativa, fermi restando i limiti della pertinenza, non eccedenza e completezza delle informazioni, rispetto agli scopi considerati.
Il personale che tratta i dati personali è incaricato dello svolgimento delle singole operazioni con istruzioni scritte e può avere accesso alle informazioni che siano strettamente necessarie allo svolgimento dei compiti assegnati.
Lei potrà far valere i propri diritti come espressi dagli artt. 7, 8, 9 e 10 del D. Lgs. 30 giugno 2003 n. 196, presentando istanza ad uno dei Responsabili del Trattamento, richiedendo l'apposito modulo all'URP o all'indirizzo sopra riportato.
Titolare del Trattamento è il COMUNE DI RAGUSA.
Luogo e data

Modello n. 4 – Informativa per la selezione del personale

In osservanza di quanto previsto dal D. Lgs. 30 giugno 2003 n. 196, La informiamo che per quanto riguarda la tutela dei dati personali il COMUNE DI RAGUSA. ha provveduto ad adottare gli adempimenti necessari stabiliti, dal D.Lgs. 196/03 in "materia di protezione dei dati personali" al fine di migliorare l'offerta dei propri servizi e di garantire la tutela della riservatezza dei propri utenti.

Tali documenti sono in visione presso l'URP o presso i singoli Settori.

Desideriamo informarLa che i dati personali che sono stati raccolti con la domanda di partecipazione e il curriculum vitae sono trattati esclusivamente per finalità di selezione del personale e per l'espletamento delle relative procedure concorsuali.

I dati sono trattati sia con mezzi cartacei, sia automatizzati, nel rispetto delle regole previste dalla legge sulla privacy e adottando specifiche misure di sicurezza. Il conferimento dei dati necessari alla partecipazione alle procedure di selezione o concorsuali è necessario, pena l'esclusione o la non ammissione. Al contrario i curricula e ogni altro elemento ritenuto utile può essere facoltativamente allegato alla domanda di partecipazione, ai fini della valutazione da parte della commissione esaminatrice, ai cui membri (solamente) le informazioni personali dei partecipanti sono comunicate. A conclusione delle procedure, la graduatoria di merito viene affissa all'albo pretorio dell'ente. Esaurite le procedure di concorso la documentazione personale presentata può essere ritirata previa richiesta all'Ufficio personale.

La informiamo altresì che Lei può esercitare i diritti, di cui all'art. 7, presentando istanza ad uno dei Responsabili del Trattamento, richiedendo l'apposito modulo all'URP o all'indirizzo sopra riportato.

In particolare la legge, in qualità di interessato, Le consente di:

accedere alle informazioni che la riguardano e conoscere le finalità e le modalità del trattamento, nonché la logica dello stesso;

chiedere la cancellazione, il blocco o la trasformazione in forma anonima dei dati trattati in violazione della legge;

opporsi al trattamento per motivi legittimi;

chiedere l'aggiornamento, la rettificazione o, qualora ne abbia interesse, l'integrazione dei dati trattati.

Titolare del Trattamento è il COMUNE DI RAGUSA.

Modello n. 5 – Informativa Procedure appalti

In osservanza di quanto previsto dal D. Lgs. 30 giugno 2003 n. 196, siamo a informarLa che per quanto riguarda la tutela dei dati personali il COMUNE DI RAGUSA ha provveduto ad adottare gli adempimenti necessari stabiliti dal D.Lgs. 196/03 in "materia di protezione dei dati personali" al fine di migliorare l'offerta dei propri servizi e di garantire la tutela della riservatezza dei propri utenti.

Tali documenti sono in visione presso l'URP o presso i singoli Dirigenti di Settore.

Il Comune di Ragusa informa le imprese, associazioni, cooperative e i prestatori d'opera professionale o manuale che i dati richiesti con il bando o con la lettera di invito sono trattati esclusivamente per finalità di selezione delle offerte ai fini della scelta dei contraenti, cui aggiudicare la fornitura o l'esecuzione dei servizi richiesti.

I dati vengono comunicati esclusivamente ai membri della commissione giudicatrice, nominata all'uopo, per lo svolgimento delle procedure di appalto ovvero per le gare informali.

Le informazioni che possono essere trattate sono quelle espressamente previste dalla normativa comunitaria, nazionale e regionale specifica, nonché dall'atto dell'Ente, disciplinante le procedure cd. sottosoglia e dai bandi di gara o dalle lettere di invito.

Le informazioni richieste a pena di esclusione devono essere necessariamente conferite; per il resto è in facoltà del soggetto, che partecipa alle procedure selettive, presentare dati e informazioni, ritenuti utili agli scopi in oggetto, che costituiscono il limite del trattamento.

Vengono diffusi solo i dati relativi alla graduatoria finale di aggiudicazione, attraverso la pubblicazione all'albo dell'Ente.

Titolare del Trattamento è il COMUNE DI RAGUSA).

Un elenco completo e aggiornato dei responsabili del trattamento è disponibile presso l'URP oppure presso gli uffici dei singoli Settori.

La informiamo altresì che Lei può esercitare i diritti, di cui all'art. 7, presentando istanza ad uno dei Responsabili del Trattamento, richiedendo l'apposito modulo allo stesso ufficio.

In particolare la legge, in qualità di interessato, Le consente di:

accedere alle informazioni che la riguardano e conoscere le finalità e le modalità del trattamento, nonché la logica dello stesso; chiedere la cancellazione, il blocco o la trasformazione in forma anonima dei dati trattati in violazione della legge;

opporsi al trattamento per motivi legittimi;

chiedere l'aggiornamento, la rettificazione o, qualora ne abbia interesse, l'integrazione dei dati trattati.