ALLEGATO A

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(DECRETO LEGISLATIVO 30 GIUGNO 2003, n. 196)

TITOLARE DEL TRATTAMENTO DEI DATI: COMUNE DI ANCONA

Rif. int. : DPS

File : DPS_COMUNE_DI_ANCONA.doc

Creatore :

Approvazione : Commissario straordinario

Data :

Premessa

Nel corso degli anni le attività istituzionali svolte dagli uffici del Comune di Ancona sono svolte utilizzando sempre di più le tecnologie dell'informazione e della comunicazione ICT (Information & Communication Technology).

Per questo motivo viene chiesto un elevato grado di disponibilità, affidabilità e sicurezza informatica in relazione agli strumenti elettronici e ai dati oggetto di trattamento.

Considerate però le caratteristiche di apertura che i moderni sistemi informativi presentano nei confronti del mondo esterno all'Amministrazione - ad esempio l'utilizzo abituale della rete Internet come strumento di ausilio nella ricerca di informazioni e di facilitazione nell'interscambio informativo con altri soggetti – l'attuale stato dell'arte della tecnologia ICT considera i sistemi informativi come oggetti potenzialmente esposti a diversi rischi legati alle intrusioni informatiche, cioè alla possibilità che persone non autorizzate possano ottenere un qualche tipo di accesso agli archivi presenti sui sistemi gestiti dal Comune.

Il Comune di Ancona, in ottemperanza a quanto previsto dall'art. 34 del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e dal punto 19 dell'allegato B al codice, redige ed aggiorna con cadenza annuale un documento programmatico sulla sicurezza (DPS).

In sede di aggiornamento, si è previsto di implementare e modificare la struttura del DPS, che attualmente risulta composto da:

1) articolato (adottato con deliberazione di Giunta municipale), contenente la determinazione degli indirizzi, dei criteri e dei compiti per l'adozione e il controllo delle misure di sicurezza degli strumenti e dei dati;
2) allegati sotto elencati (da approvarsi con successiva determinazione, in esecuzione e adempimento degli indirizzi impartiti dalla Giunta e dal Sindaco, secondo le funzioni e i compiti riportati all'articolo 6 dell'articolato).

    - ELENCO DEI TRATTAMENTI DEI DATI PERSONALI, DELLE BANCHE DATI CENTRALI E LOCALI E DEI RESPONSABILI INTERNI ED ESTERNI DEL TRATTAMENTO;
    - EVENTI A RISCHIO
    - SALVATAGGIO E RIPRISTINO
    - ANALISI DEI RISCHI E PIANIFICAZIONE DELLE MISURE INFORMATICHE
    - ARCHITETTURA DI SISTEMA

Per quanto riguarda le misure di sicurezza relative al sistema informatico del Comune di Ancona si è ritenuto opportuno adottare separatamente apposito "REGOLAMENTO RELATIVO ALL'ACCESSO E ALL'USO DELLA RETE INFORMATICA E TELEMATICA DEL COMUNE DI ANCONA" (delibera di Giunta n. 823 del 29/12/2005). Il documento, redatto dal Servizio Sistemi Informativi, per il suo specifico contenuto è comunque da intendersi strettamente collegato al presente documento.

DISPOSIZIONI GENERALI
Articolo 1 – Finalità e oggetto del presente documento

*Il presente documento individua indirizzi, criteri generali e modalità applicative relative all'adozione delle misure di sicurezza a protezione dei dati personali oggetto di trattamento da parte del Comune di Ancona, in qualità di titolare, secondo quanto previsto dal Decreto Legislativo del 30 Giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*", di seguito per brevità denominato "Codice".*

I responsabili e gli incaricati del trattamento dei dati, designati ai sensi degli articoli 29 e 30 del Codice provvedono all'esercizio delle funzioni e allo svolgimento dei compiti e delle operazioni, nel rispetto delle istruzioni scritte ricevute e, in generale, delle disposizioni specifiche del Codice e della normativa di settore, a seconda dell'ambito di trattamento di competenza.

Il presente documento si applica a tutti i soggetti che operano trattamenti di dati personali per conto del titolare, il Comune di Ancona, ai sensi del D.Lgs. 30 giugno 2003, n. 196.

Articolo 2 – Definizioni

Ai fini del presente documento si riportano le definizioni dettate dall'art. 4, comma 1, del Codice e, con riferimento alla definizione di "amministratore di sistema", dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008" (G.U. n. 300 del 24.12.2008)*:*

a) "**trattamento**", 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 di dati, anche se non registrati in una banca di dati;

b) "**dato personale**", qualunque informazione relativa a 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;

c) "**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;

d) “**dati sensibili**”, 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;

e) “**dati giudiziari**”, i dati personali idonei a rivelare provvedimenti di cui all’articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 213, 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 articoli60 e 61 del codice di procedura penale;

f) "**titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) “**incaricati**”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) “**amministratore di sistema**”, le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini dell’applicazione del provvedimento del Garante del 27 novembre 2008, vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

l) "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

m) "**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;

n) "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

o) "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

p) "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

q) “**banca di dati**”, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

r)"**Garante**", l'autorità di cui all’articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Si riportano, inoltre, le ulteriori definizioni di cui all’art. 4, comma 2, del predetto Decreto Legislativo:

a) “**comunicazione elettronica**”, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) “**chiamata**”, la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) “**reti di comunicazione elettronica**”, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) “**rete pubblica di comunicazioni**”, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) “**servizio di comunicazione elettronica**”, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall’articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

m) “**posta elettronica**”, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell’apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Si riportano infine le ulteriori definizioni di cui all’art. 4, comma 3, del predetto Decreto Legislativo:

a) "**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 nell'articolo 31;

b) "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;

e) "**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;

f) "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) "**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.

Articolo 3 – Modalità di trattamento dei dati

I dati personali devono essere trattati nel rispetto dei principi generali e delle modalità stabilite dall'articolo 11 del Codice.

Nel caso di trattamenti svolti con strumenti elettronici, una particolare cura deve essere prestata al rispetto delle disposizioni e degli obblighi previsti dagli articoli 3 e 22 del Codice, rispettivamente disciplinanti il principio di necessità e di indispensabilità del trattamento dei dati sensibili e giudiziari rispetto alle finalità da perseguire in concreto.

Le disposizioni del presente documento si applicano, in quanto compatibili, al trattamento dei dati svolto anche senza l'ausilio di strumenti elettronici.

Articolo 4 – Informativa

Il responsabile e l'incaricato del trattamento dei dati, che procedano alla raccolta delle informazioni, devono fornire idonea informativa all'interessato, sia in forma orale, sia – preferibilmente - per iscritto, utilizzando la modulistica specifica redatta in sede di implementazione del DPS, disponibile in intranet e pubblicata sul sito internet dell'ente.

I modelli di informativa, predisposti ai sensi dell'art. 13 del Codice, devono essere oggetto di analisi e adeguamento, apportando le modificazioni ed integrazioni, da parte dei singoli responsabili del trattamento, ovvero degli incaricati a ciò delegati, in modo da garantire idonea e completa informazione, fornendo ogni ulteriore chiarimento a richieste degli interessati.

Articolo 5 – Diritti dell'interessato ai sensi dell'art. 7 del Codice.

L'esercizio dei diritti da parte degli interessati, ai sensi dell'art. 7 del Codice, possono essere presentate direttamente all'Ufficio Comunicazione e Rapporti con i cittadini del Comune di Ancona ovvero al responsabile del trattamento competente, utilizzando la modulistica disponibile sul sito internet del Comune ovvero facendone richiesta diretta agli uffici competenti.
Il responsabile del trattamento, ovvero la persona a ciò incaricata, deve dare idoneo riscontro all'interessato senza ritardo, e comunque entro e non oltre il termine di 15 giorni dal ricevimento dell'istanza di interpello.
In deroga a quanto previsto al comma precedente, il termine può essere di 30 giorni se le operazioni per dare un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo ai sensi dell'art. 146, commi 2 e 3 del Codice. In queste ipotesi occorre dare previa comunicazione all'interessato dei motivi.

La Giunta Comunale determina con apposito atto il contributo spese a carico del richiedente, se dovuto, ai sensi dell'art. 10 del Codice.

Articolo 6 – Funzioni e compiti per il trattamento dei dati e la sicurezza e protezione degli strumenti e delle informazioni

Il Titolare dei dati, ai sensi dell'art. 28 del Codice, è il Comune di Ancona nella persona del legale rappresentante, ovvero del Sindaco pro-tempore.

Il Titolare dei dati nomina il Responsabile del trattamento dei dati con provvedimento motivato, sulla base di quanto previsto dall'art. 29 del D.Lgs. 30 Giugno 2003 n.196.

Il Comune di Ancona, dotato di una struttura organizzativa articolata e complessa, per esigenze organizzative ha deciso di individuare più Responsabili del trattamento dati, nelle persone del Segretario Generale, il Direttore Generale, i Direttori di Area e di progetto e Dirigenti pro tempore dei Settori nei quali è articolato il Comune di Ancona, ai sensi del Regolamento di organizzazione delle Dirigenza.

Il Comune di Ancona ha individuato, con decreto sindacale, i responsabili del trattamento nelle persone dei dirigenti pro-tempore di aree e servizi, ai quali sono assegnati compiti, da ascrivere a tre diverse tipologie:

a) **natura amministrativa:** compiti di gestione e organizzazione dei trattamenti, attribuiti ai dirigenti di servizio;
b) **natura tecnica:** concernenti profili di natura informatica e della sicurezza e protezione degli strumenti e dei dati, assegnati al dirigente e al personale del Settore Informatica e Innovazione;
c) **funzioni di controllo e di vigilanza:** nell'ottica di implementazione di un sistema di gestione, fondamentali appaiono anche le attività di audit collaborativi, che possono essere assegnate a dirigenti e a personale in posizione di terzietà.

A) Compiti di natura amministrativa:

Responsabilità	Attività
I-Settore Personale e organizzazione: Ufficio Coordinamento privacy	1. fornire gli indirizzi operativi ai responsabili del trattamento per l'attuazione degli adempimenti necessari; 2. aggiornare, con atto dirigenziale gli ALLEGATI del Documento Programmatico sulla Sicurezza (DPS) secondo le funzioni e compiti di cui al presente articolo: - Elenco dei trattamenti dei dati personali, delle banche dati centrali e locali e dei responsabili interni ed esterni, recependo con atto amministrativo gli aggiornamenti provenienti dai Responsabili del trattamento dati e dal Dirigente del Settore Informatica e Innovazione; 3. aggiornare il Regolamento sui dati sensibili e giudiziari; 4. coordinare l'attività di monitoraggio del processo di trattamento, al fine dell'aggiornamento del documento programmatico sulla sicurezza (DPS); 5. segnalare eventuali necessità di formazione/ informazione degli incaricati in tema di tutela della riservatezza dei dati personali e sensibili e protezione degli strumenti elettronici e degli archivi; 6. fornire indirizzi per redigere l'informativa agli interessati, nei casi e con le modalità previsti dall'art. 13 codice privacy; 7. fornire indirizzi operativi per il riscontro delle istanze presentate dagli interessati ai sensi dell'art. 7 del codice privacy; 8. rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito dell'organizzazione quando la loro attività riguardi anche indirettamente servizi o sistemi che trattano o permettono il trattamento di informazioni di carattere personale di lavoratori.
II- Settore Informatica e	1. aggiornare il Documento Programmatico sulla Sicurezza (DPS) per le parti di competenza :

Innovazione	- trasmissione all'Ufficio Coordinamento Privacy delle parti di propria competenza relative all'ALLEGATO "Eventi e rischio" ; - di predisporre un documento che contenga le "Misure attuative sugli amministratori di sistema" e di procedere alla loro nomina ai sensi dei provvedimenti del Garante per la protezione dei dati personali del 27.11.2008 e 25.06.2009; - trasmissione all'Ufficio Coordinamento privacy dell'elenco aggiornato degli Amministratori di sistema; - comunicazione all'ufficio Coordinamento privacy degli estremi dell'atto dirigenziale di approvazione/aggiornamento degli ALLEGATI di competenza del Settore, previsti tra i compiti di natura tecnica
III- Responsabili del trattamento	*1. aggiornare il Documento Programmatico sulla Sicurezza (DPS) per le parti di competenza:* *a)trasmissione all'Ufficio Coordinamento Privacy dell'elenco aggiornato dei trattamenti dati di propria competenza , nonché dei soggetti nominati/da nominarsi Responsabili esterni,ai sensi dell'art. 13 del presente documento, al fine dell'aggiornamento dell'ALLEGATO "Elenco dei trattamenti dei dati personali, delle banche dati centrali e locali e dei Responsabili interni ed esterni del trattamento";* b)trasmissione all'Ufficio Coordinamento Privacy delle parti di competenza relative all'ALLEGATO "Eventi e rischio"; *2. attuare gli indirizzi dell'Ufficio Coordinamento, al fine di:* *a)provvedere all'adozione di idonee procedure organizzative;* *b)omogeneizzare i comportamenti degli incaricati del trattamento, idonei a garantire la protezione dei dati personali e la tutela della riservatezza dei dati;* *3. procedere all'attività di monitoraggio del processo di trattamento dei dati personali;* *4. aggiornare periodicamente i trattamenti di competenza del proprio settore al fine di darne comunicazione all'Ufficio Coordinamento privacy per l'aggiornamento del DPS (punto 1. a);* *5. determinare, in via eventuale, a seconda dell'organizzazione del proprio servizio, la ripartizione dei compiti, anche per classi omogenee o gruppi di lavoro, da affidare agli incaricati con i relativi profili di autorizzazione ai trattamenti;* *6. individuare gli incaricati del trattamento consegnando la "lettera generale di incarico - Istruzioni per l'incaricato", corredata delle apposite istruzioni, e la determinazione dei compiti specifici secondo la determinazione di cui al n.5);* *7. richiedere l'attivazione/disattivazione/variazione del profilo di autenticazione e di autorizzazione del personale che opera*

	all'interno dell'area – servizio di propria competenza, utilizzando la modulistica fornita dal Servizio Sistemi Informativi; *8. aggiornare periodicamente gli Eventi a rischio e i Responsabili esterni del trattamento relativi al proprio settore al fine di darne comunicazione all'Ufficio Coordinamento privacy per l'aggiornamento del DPS (punti 1.c e 1.a)* *9. interagire con il Coordinamento per pianificare la formazione/informazione degli incaricati in tema di tutela della riservatezza dei dati personali e sensibili;* *10. verificare che gli incaricati operanti in attività di front-office forniscano l'informativa, nel rispetto delle procedure e utilizzando gli appositi moduli predisposti dall'ente, ai sensi dell'art. 13;* *11. adottare idonee procedure per garantire il riscontro delle istanze presentate dagli interessati ai sensi dell'art. 7 del codice privacy, procedendo ad individuare un incarico preposto al relativo riscontro;* *12. vigilare sull'attività degli incaricati preposti ad operare presso l'Unità di appartenenza, anche mediante la programmazione di visite ispettive.*

B) Compiti di natura tecnica:

Responsabilità	Attività
I- Settore Informatica e Innovazione	1. redigere, aggiornare e custodire la documentazione relativa agli ALLEGATI: • "Salvataggio e ripristino" • "Analisi dei rischi e pianificazione delle misure informatiche" • "Architettura di sistema"; 2. Al dirigente del Settore Informatica e Innovazione è affidato il ruolo di Amministratore del Sistema Informatico Comunale , con il compito di: • adottare i provvedimenti necessari alla protezione dei dati trattati con strumenti elettronici, • sovraintendere alle attività degli Amministratori di sistema, • pianificare la formazione del personale del Settore Informatica e Innovazione, in materia di soluzioni tecniche per la garanzia della sicurezza dei dati e della protezione degli strumenti elettronici, • adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli

	Amministratori di sistema. 3. Ulteriori compiti tecnici sono: • gestire le credenziali di autenticazione dei responsabili e dei soggetti incaricati del trattamento; • gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili del trattamento; • provvedere alla disattivazione/variazione delle utenze assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili; • seguire misure necessarie ad evitare la perdita o la distruzione dei dati presenti sui server e provvedere al loro salvataggio periodico con copie di back-up secondo criteri stabiliti; • assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro e del loro ripristino in caso di necessità; • fare in modo che sia prevista la disattivazione dei "codici identificati personali" (User-ID), in caso di perdita della qualità di incaricato all'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei "codici identificativi personali" (User-ID) per un periodo superiore a 3 mesi; • proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi aggiornati almeno ogni 6 mesi; • mantenere un adeguato sistema di autorizzazione che, per ogni identificativo utente, riporti la data di attivazione, le funzioni del sistema alle quali l'utente è abilitato, la data di cessazione dell'identificativo stesso; • registrare e archiviare le attività eseguite sul sistema secondo le necessità operative nel rispetto della normativa sul trattamento dei dati e sulla tutela della riservatezza dei lavoratori all'interno dei luoghi di lavoro; • garantire che le informazioni scambiate con soggetti interni ed esterni siano opportunamente protette da rischi di intrusione. Il Dirigente del Settore Informatica e Innovazione ha, inoltre, il compito di definire e verificare che i fornitori di strumenti elettronici garantiscano che: • l'hardware sia conforme alla normativa in materia di protezione dei dati personali, con particolare riferimento al rispetto del principio di necessità, di cui all'art. 3 del codice privacy, e che, in occasione di ciascun intervento di manutenzione e di assistenza tecnica, sottoscrivano un verbale sulla esecuzione dei lavori, che attesti la conformità alle regole dette o rilascino una dichiarazione di conformità

	ai sensi dell'art.25 all.B del codice della privacy. • i software operativi e i programmi applicativi siano idonei ad assicurare: - la separazione tra dati anagrafici e dati sensibili, ovvero la cifratura dei dati idonei a rivelare lo stato di salute, ai sensi dell'art. 22, comma 6 e del punto 24 dell'allegato B del codice privacy; - la tracciabilità delle attività degli utenti, nel rispetto del codice privacy e delle garanzie di tutela dei dipendenti; - un sistema di autenticazione e di autorizzazione conforme alla normativa in materia di protezione dei dati personali;
II- Responsabili di banche dati locali	I Responsabili del trattamento hanno la responsabilità dell'applicazione delle misure di sicurezza in caso di utilizzo di banche dati locali (file excel, access ecc.), ubicate sulle postazioni di lavoro in uso presso gli uffici. Poiché questi archivi devono essere sottoposti ad idonee misure di sicurezza, al fine di agevolare l'operato dei responsabili del trattamento e della vigilanza sull'applicazione della normativa, vengono di seguito indicate le regole di gestione, back-up e ripristino delle banche dati informatiche locali. Queste regole non sostituiscono, ma integrano e completano quelle già indicate nel regolamento interno per l'applicazione della normativa sulla privacy e per l'uso degli strumenti informatici . (Procedura Operativa per la gestione degli accessi al Sistema Informativo Comunale - Regolamento relativo all'accesso e all'uso della rete informatica e telematica del comune di Ancona) Regole di gestione back-up e ripristino banche dati informatiche locali: 1. individuare e descrivere le banche dati locali, in termini di: a. correttezza del trattamenti previsti, la pertinenza e la non eccedenza dei dati rispetto alle finalità del loro trattamento; b. contenuto e natura dei dati (comuni, sensibili, giudiziari); c. interessati al trattamento (cittadini, dipendenti, fornitori); 2. verificare la possibilità e definire le modalità per il passaggio della banca dati ad una gestione centralizzata; 3. effettuare almeno ogni sei mesi la pulizia degli archivi, con cancellazione dei file obsoleti o inutili; evitare un'archiviazione ridondante; evitare la duplicazione di parti di banche dati gestite centralmente 4. prevedere l'accesso alle banche dati attraverso userid e password; le password devono: a. essere lunghe almeno 8 caratteri, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili)

	b. avere una durata massima di 6 mesi, trascorsi i quali le password devono essere sostituite, in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi c. deve essere immediatamente sostituita, nel caso si sospetti che la stessa abbia perso la segretezza 5. verificare, almeno una volta all'anno, la sussistenza delle condizioni per la conferma della autorizzazioni al trattamento da parte degli incaricati; evitare che permangano permessi non necessari nel caso di cambio mansioni. 6. prevedere la crittografia delle banche dati nel caso queste contengano dati sensibili e giudiziari 7. effettuare con frequenza settimanale, copie di salvataggio delle banche dati; custodire le copie in armadio chiuso a chiave in un locale diverso da quello dove avviene il trattamento dei dati 8. effettuare ogni tre mesi prove di ripristino dei dati salvati 9. impedire l'accesso sia fisico che logico alla postazione di lavoro agli estranei al trattamento; nel caso di banche dati contenenti dati sensibili e giudiziari, l'accesso ai locali e al trattamento, oltre il normale orario di lavoro, deve essere preventivamente autorizzato dal responsabile del trattamento e documentato. 10. limitare la copia di dati su supporti rimovibili; tutti i supporti riutilizzabili contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato 11. nel caso di banche dati presenti su postazioni NON collegate alla rete locale a. installare ed aggiornare almeno con frequenza settimanale una protezione antivirus b. proteggere la postazione di lavoro con userid e password c. applicare gli aggiornamenti al software di sistema e applicativo d. proteggere con gruppo di continuità elettrica la postazione di lavoro 12. nel caso di banche dati presenti su postazioni collegate alla rete locale SE tali banche dati vengono installate su di una cartella di rete (file server) non è necessario applicare le disposizioni n.7 e n.11.a, 11.b, 11.c, di competenza del Settore Informatica e Innovazione, previa valutazione della effettiva fattibilità tecnica. Nel caso di valutazione positiva è obbligatorio da parte del responsabile, rendere noto al Settore Informatica e Innovazione: a) la descrizione della banca dati di cui al punto 1. prima della effettiva installazione, b) tempestivamente tutte le modifiche apportate a quanto comunicato al punto precedente. 13. aggiornare periodicamente le banche dati locali secondo le regole tecniche sopra elencate.

C) Funzioni di controllo e di vigilanza:

Responsabilita'	Attività
I- Responsabili del trattamento	1.verificare l'adozione delle misure minime di sicurezza; 2. verificare lo stato di adozione delle misure idonee di sicurezza; 3. verificare gli eventi che hanno causato rischi per l'integrità e la disponibilità dei dati personali; 4. redigere una relazione da presentare al coordinamento privacy dell'ente, entro il 28 febbraio di ciascun anno, al fine di consentire l'aggiornamento del DPS;
II- Ufficio coordinamento privacy	1.verificare il rispetto delle istruzioni per il trattamento impartite ai responsabili del trattamento;
III- Servizio Sistemi Informativi	1.pianificare regolari controlli della vulnerabilità dei programmi per elaboratore; 2. verificare, almeno una volta all'anno, l'operato degli Amministratori di sistema ai sensi del Provvedimento del Garante 27.11.2009 e di quanto previsto nel documento che contiene le "Misure attuative sugli Amministratori di sistema";

Articolo 7 – Analisi dei rischi

L'analisi dei rischi deve essere svolta utilizzando la tabella con l'elenco delle minacce e delle vulnerabilità (ALLEGATO).

La metodologia usata è quella suggerita dal documento del Garante dell'11 giugno 2004 "Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)" e dagli standard internazionali BS7799.

Articolo 8 – Misure di sicurezza

Le misure di sicurezza relative al trattamento dei dati personali effettuate con strumenti elettronici, così come individuate e definite nell'art.3 da adottare per garantire l'integrità e la disponibilità dei dati stessi sono di seguito riportate:

10.1 Sistema di autenticazione informatica

Il sistema informativo del Comune di Ancona consente solo agli incaricati dotati di appropriate credenziali il superamento di una procedura di autenticazione per accedere ad uno specifico trattamento o ad un insieme di trattamenti a seconda dei diritti assegnati agli incaricati stessi.
Le credenziali di autenticazione consistono in un codice univoco composto da un nome utente (username) ed una parola chiave riservata e conosciuta solamente dal medesimo (password).
L'accesso alla rete è univoco, ma esistono diverse credenziali a seconda del trattamento e dell'applicazione utilizzata (conosciute però solo dall'utente stesso).

Esiste un regolamento e specifiche procedure operative di utilizzo delle attrezzature informatiche attraverso le quali vengono impartite idonee istruzioni per garantire la segretezza della componente riservata della credenziale.
Le disposizioni relative alle parole chiavi (componenti riservate del codice di autenticazione) sono specificate nel regolamento.
Le credenziali degli utenti non più in servizio sono disabilitate e non più utilizzabili.
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali di autenticazione verranno disattivate anche nel caso in cui l'utente cambi mansioni e quindi non abbia più titolarità ad accedere a trattamenti per i quali era stato precedentemente incaricato.
Nel regolamento di utilizzo delle attrezzature informatiche sono date istruzioni al personale volte a non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
Nel regolamento di utilizzo delle attrezzature informatiche sono date istruzioni al personale volte a 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 particolare gli amministratori di sistema, su richiesta del dirigente di struttura dell'utente assente o impedito, procederanno alla reinizializzazione della parola chiave che dovrà essere nuovamente impostata dall'utente al suo ritorno.

10.2 Sistema di autorizzazione

Il sistema di autorizzazione utilizzato dal Comune di Ancona consente la creazione di profili di autorizzazione per ciascun incaricato.
Attualmente 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.
I dirigenti di servizio e/o l'ufficio personale, verificheranno annualmente sulla sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

10.3 Altre misure per trattamento con elaboratori elettronici

Il sistema di autorizzazione utilizzato dal Comune di Ancona permette di includere le credenziali di ciascun utente in gruppi di dominio caratterizzati da classi omogenee di profili di autorizzazione.
Viene utilizzato un sistema antivirus che permette un controllo ed una scansione centralizzata della presenza di programmi di cui all'art. 615-quinquies del codice penale; l'aggiornamento delle firme virali avviene in tempo reale non appena le suddette firme sono rese disponibili dalla casa produttrice del software antivirus e, in ogni caso, con cadenza almeno semestrale.
Il Sistema informatico è dotato di un sistema in grado di installare automaticamente gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità di

strumenti elettronici e a correggerne i difetti; l'aggiornamento avviene in ogni caso almeno con cadenza annuale o semestrale in caso di dati sensibili o giudiziari.
Il salvataggio dei dati è effettuato con cadenza giornaliera (salvataggio completo con cadenza settimanale e differenziale giornaliero) in via centralizzata dal Servizio Sistemi Informativi. Al personale sono date istruzioni e vengono forniti gli strumenti per archiviare i file contenenti dati personali all'interno di cartelle di rete fisicamente presenti sui server sui quali viene eseguito il salvataggio descritto sopra.

10.4 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

I dati sensibili e giudiziari sono custoditi nelle cartelle condivise sui file server ai soggetti gestiti all'interno di specifici gruppi omogenei che ne hanno l'accesso; le politiche di condivisione di questi dati sono realizzate su richiesta del dirigente.
I supporti magnetici utilizzati per il salvataggio dei dati presenti sui server sono custoditi in un locale diverso dalla sala server con accesso controllato.

Il salvataggio dei dati sensibili o giudiziari è effettuato con le stesse modalità descritte al punto 10.3 al comma 4 .

10.5 Misure di tutela e garanzia

Il Comune di Ancona richiede ai soggetti esterni che effettuano interventi che possono incidere sulle misure minime di sicurezza una dichiarazione di conformità alle disposizioni del disciplinare allegato B al Dlgs 196/2003.
Ogni anno in occasione della stesura della relazione accompagnatoria del bilancio d'esercizio viene inserito il riferimento alla redazione o all'aggiornamento del Documento Programmatico di Sicurezza.

Articolo 8 bis – Amministratori di sistema

Ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema", il Responsabile designa quali amministratori di sistema definiti alla lett. i) dell'art. 2 del presente documento, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, i dipendenti individuati ai sensi dell'art. 30 del Codice, in qualità di incaricati del trattamento.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni personali dei lavoratori, viene resa nota o conoscibile l'identità degli amministratori di sistema mediante circolare, pubblicazione nella intranet del Comune di Ancona e, ove necessario, tramite apposita informativa ai sensi dell'art. 13 del DPS.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing, vengono conservate direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

L'operato degli amministratori di sistema è soggetto, con cadenza almeno annuale, ad una attività di verifica in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

L'Amministrazione comunale soddisfa la misura relativa alla verifica delle attività e registrazione dei accessi (punti 4.4 e 4.5 provvedimento del Garante del 27 novembre 2008) mediante l'adozione di un sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni devono avere carattere di completezza, inalterabilità e possibilità di verifica della loro integrità e devono comprendere i riferimenti temporali e la descrizione dell' evento che le ha generate e devono essere conservate per un periodo non inferiore ai sei mesi.

Articolo 9 – Trattamenti senza l'ausilio di strumenti elettronici

Gli incaricati del trattamento di dati personali devono provvedere ad un adeguato controllo e custodia degli atti e documenti loro affidati, nel rispetto di quanto previsto dalle istruzioni riportate nella lettera di incarico.

Nel caso in cui i documenti o gli atti contengano dati sensibili o giudiziari il responsabile del trattamento deve impartire ulteriori direttive al fine di prescrivere quanto necessario per una idonea custodia dei documenti e degli atti affidati agli incaricati per l'intera durata del trattamento, in modo che non vi possano accedere persone prive di autorizzazione.

Al termine delle operazioni, l'incaricato deve riporre i documenti e gli atti nell'archivio individuato da ciascun responsabile.

I documenti contenenti dati sensibili e giudiziari vanno archiviati in armadi o contenitori fisicamente separati da quelli che contengono dati comuni, in modo tale che non possano accedervi soggetti non espressamente incaricati.

L'accesso agli archivi, che contengono dati sensibili o giudiziari, è sorvegliato e consentito solo a persone espressamente autorizzate secondo modalità appositamente disciplinate dal Responsabile del trattamento e finalizzate ad identificare gli incaricati. Dopo l'orario di lavoro, invece, per l'accesso occorre oltre all'autorizzazione di cui sopra anche essere identificati e registrati.

Articolo 10 – Misure di sicurezza per la carta di identità elettronica (CIE)

Il Comune di Ancona, per l'emissione delle carte di identità elettroniche, si avvale delle seguenti infrastrutture di sicurezza:
• Backbone di Sicurezza del CNSD e Porta di accesso ai domini applicativi del CNSD

presente presso l'infrastruttura Comunale.
• Sistema di Sicurezza del Circuito di Emissione delle carte d'identità e dei documenti
d'identità elettronici.

La sicurezza viene gestita sia nelle reti di comunicazioni dati, sia per tutti gli apparati inerenti alla struttura comunale di emissione ed uso della CIE, sia per il materiale di consumo considerato sensibile.

Le misure di sicurezza per la CIE adottate dal Comune di Ancona sono descritte nel Piano della Sicurezza Comunale CIE.

Articolo 11 – Salvataggio e ripristino dei dati

I criteri e le procedure adottati per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati sono descritti in apposito allegato, approvato con determinazione da parte del Responsabile del Servizio Sistema Informativo.

Articolo 12 – Formazione e addestramento

Il Comune di Ancona prevede interventi formativi sia per i Responsabili del Trattamento, sia per gli Incaricati del trattamento che sono inclusi nel piano della formazione, secondo le richieste presentate dai singoli responsabili all'Ufficio di Coordinamento.

La formazione deve avere ad oggetto i rischi che incombono sui dati, le misure disponibili per prevenire eventi dannosi, i profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, le responsabilità che ne derivano e le modalità per aggiornarsi sulle misure minime adottate dal Comune.

Articolo 13 – Trattamenti affidati a soggetti esterni all'organizzazione del Comune

I soggetti esterni all'organizzazione del Comune sono nominati responsabili del trattamento, nelle ipotesi in cui non vi sia una espressa previsione di legge o di regolamento, che autorizzi la comunicazione o la diffusione dei dati raccolti e trattati dal Comune di Ancona, in qualità di titolare.

Il Sindaco, in qualità di legale rappresentante dell'ente, titolare del trattamento nel suo complesso, con proprio decreto nomina il responsabile esterno del trattamento, secondo quanto previsto dall'art. 29 del Codice e nei casi di cui al comma precedente.

Al responsabile esterno del trattamento devono essere assegnati con decreto sindacale i compiti e impartite idonee istruzioni scritte, omogenee, in quanto compatibili, a quelle in uso per i responsabili e gli incaricati interni.

Al fine di garantire l'adozione delle misure minime di sicurezza, a ciascun soggetto nominato responsabile esterno del trattamento è richiesto lo stesso livello di tutela per i dati trattati all'interno dell'ente; perché sia garantito un adeguato trattamento dei dati è necessario che il soggetto esterno a cui viene affidato il trattamento assuma impegni sia in sede contrattuale ovvero con eventuale accordo accessorio al contratto.

Il soggetto, nominato responsabile esterno del trattamento, deve dichiarare:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto sono nella titolarità del Comune e che possono essere tratti solamente per lo svolgimento delle funzioni e dei compiti affidati;
2. di ottemperare agli obblighi previsti dal Codice e dall'allegato B al Codice medesimo;
3. di individuare gli incaricati e di assegnare istruzioni scritte specifiche;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di comunicare immediatamente al Comune eventuali situazioni di anomalia o di non conformità a quanto previsto dal Codice o dalle istruzioni ricevute;
5. di riconoscere al personale incaricato dal Comune la facoltà di verificare periodicamente il rispetto delle istruzioni, nonché l'applicazione delle norme di sicurezza adottate.

Un elenco completo indicante i soggetti, che sono stati nominati in qualità di responsabili del trattamento, è tenuto ed aggiornato a cura dell'Ufficio di Coordinamento, su segnalazione dei responsabili, ciascuno di propria competenza, ai sensi dell'art. 6 del presente articolato.