

## LA GIUNTA DELLA REGIONE EMILIA-ROMAGNA

Visto il Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione di dati personali”, di seguito indicato come Codice;

Rilevato che il Codice non solo riordina in un unico testo la normativa statale in materia di protezione dei dati personali succedutasi nel tempo ma provvede anche al suo aggiornamento sulla base dei principi giurisprudenziali e dei provvedimenti del Garante per la protezione dei dati personali approvati in attuazione della Legge n. 675/1996 e successive modifiche, nonché aggiorna tale normativa dando un assetto organico alla materia ed operando alcune semplificazioni ed adegua le misure minime di sicurezza previste a protezione dei dati personali in base al progresso tecnologico;

Valutato che la tutela del patrimonio delle informazioni riveste importanza strategica per la Giunta della Regione Emilia-Romagna, oltre che essere soggetta a precisi vincoli di legge imposti dal Codice;

Considerato che la Giunta della Regione Emilia-Romagna ha nel corso degli anni dato attuazione alla normativa statale in materia di protezione dei dati personali sia con atti del Comitato di Direzione sia con progetti specifici avviati in particolare dalla Direzione Organizzazione, Sistemi informativi e telematica - con riguardo al trattamento dei dati del personale della Giunta regionale, ai sistemi informativi ed informatici con particolare riferimento ai temi della sicurezza - e dalla Direzione Sanità e politiche sociali, con riguardo in specifico al trattamento dei dati sanitari;

Rilevato in particolare che:

- con propria deliberazione n. 960 del 27/06/2005 la Giunta regionale ha adottato la Direttiva in materia di trattamento di dati personali;
- con propria deliberazione n. 1982 del 11/10/2004 denominata “Progetto tutela della Privacy”, la Giunta regionale ha previsto la costituzione di un gruppo di progetto interdirezionale denominato “Tutela della Privacy” e che con successiva determinazione del Direttore generale Organizzazione, sistemi informativi e telematica n. 18355 del 14/12/2004 è stato costituito il gruppo di progetto suddetto;

Valutato che:

- l’impatto della normativa in materia di protezione dei dati personali coinvolge diversi aspetti dell’attività della Giunta della Regione Emilia-Romagna e tutte le sue strutture organizzative: l’attività legislativa e amministrativa, l’organizzazione, la formazione e la gestione del personale, i sistemi informativi, quelli informatici e la loro sicurezza, la rete, le attrezzature informatiche e la loro sicurezza;

- il Codice impone comportamenti rispondenti a principi tali da assicurare a chiunque il diritto alla protezione dei dati personali che lo riguardano e rende applicabili i principi di tutela in tutte le circostanze in cui, chiunque, per qualsiasi fine, tratta dati personali di soggetti terzi;
- a ciò si aggiunge il progressivo mutamento della società verso modelli di comunicazione sempre più integrati ed interconnessi (la c.d. “società dell’informazione”), che rende fondamentale per ogni organizzazione, ed a maggior ragione per un ente pubblico, lo sviluppo di una cultura della sicurezza delle informazioni e della tutela dei diritti degli interessati;
- si rende necessario assicurare maggiore organicità e coordinamento all’attività delle strutture della Giunta regionale al fine di assicurare l’attuazione della normativa in materia di tutela della privacy anche attraverso la riprogettazione di procedure e di prassi della Giunta della Regione Emilia-Romagna, l’aggiornamento del personale e l’adeguamento di modalità comportamentali nonché individuare, eventualmente, la necessità di un’attività di adeguamento dei programmi informatici e delle relative attrezzature impiegate;
- il gruppo di progetto interdirezionale denominato “Tutela della Privacy” deve elaborare indicazioni applicative del Codice anche attraverso la predisposizione di un manuale operativo *ad hoc*;
- il rispetto di quanto contenuto nel manuale operativo e nei disciplinari tecnici che ne costituiranno parte integrante, contribuisce alla riduzione dei rischi a cui i trattamenti dei dati personali possono essere sottoposti in quanto definisce i corretti comportamenti da tenere;

Per tutti i motivi sopra esposti, si ritiene necessario promuovere principi e linee guida per la diffusione nella Giunta della Regione Emilia-Romagna della cultura della sicurezza, al fine di tutelare il diritto della persona alla propria riservatezza, nel rispetto dei diritti e delle libertà fondamentali e per tutelare i diritti di accesso a tutti gli interessati;

Sentito il parere del Comitato di Direzione nella seduta del 20/06/2005;

Dato atto di aver rispettato le vigenti disposizioni in materia di relazioni sindacali;

Dato atto del parere di regolarità amministrativa espresso dal Direttore Generale all’Organizzazione, Sistemi informativi e telematica, Gaudenzio Garavini, ai sensi dell’art. 37, quarto comma, della Legge regionale n. 43/2001, della deliberazione della Giunta Regionale n. 447/2003 e della deliberazione n. 1529/2003;

Su proposta dell’Assessore a “Programmazione e sviluppo territoriale. Cooperazione col sistema delle Autonomie. Organizzazione”, Luigi Gilli;

A voti unanimi e palesi

**D e l i b e r a**

a) di approvare l'allegato "Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali" da ritenersi parte integrante del presente atto;

b) di disporre che la presente deliberazione sia pubblicata sul Bollettino Ufficiale della Regione Emilia-Romagna.

- - -

## **Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali**

### **Art. 1**

(Finalità generali)

1. Il Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione di dati personali”, di seguito indicato come Codice, impone comportamenti rispondenti a principi tali da assicurare a chiunque il diritto alla protezione dei dati personali che lo riguardano.
2. A ciò si aggiunge il progressivo mutamento della società verso modelli di comunicazione sempre più integrati ed interconnessi (la c.d. “società dell’informazione”), che rende fondamentale per ogni organizzazione, ed a maggior ragione per un ente pubblico, lo sviluppo di una cultura della protezione delle informazioni e della tutela dei diritti degli interessati.
3. Le linee guida definite in questo documento hanno come finalità il rafforzamento della sicurezza dei sistemi e delle reti di informazione e lo snellimento delle procedure per l’esercizio dei diritti degli interessati, nel rispetto dei valori di una società democratica e dell’esigenza della libertà di informazione nonché del rispetto della vita privata delle singole persone.

### **Art. 2**

(Processo di gestione della sicurezza)

1. L’applicazione ed il mantenimento della sicurezza si attuano attraverso misure tecniche e misure organizzative che devono essere recepite dai processi di lavoro per diventarne parte integrante.
2. La costruzione di un adeguato processo di gestione della sicurezza comprende le seguenti fasi distinte:
  - a) *pianificazione della sicurezza*: definizione degli obiettivi di sicurezza, analisi dei rischi, individuazione delle misure di sicurezza;
  - b) *implementazione delle misure di sicurezza*: messa in opera delle misure di sicurezza individuate;
  - c) *controlli*: verifica dell’efficienza e della corretta applicazione delle misure di sicurezza adottate;
  - d) *revisioni*: attuazione di correzioni ed adeguamenti al sistema di protezione delle informazioni sulla base dei risultati ottenuti dai controlli degli aggiornamenti normativi e tecnologici.
3. La scelta delle misure da rendere esecutive è quindi effettuata a seguito di

un'analisi costi/benefici (analisi dei rischi) e tale analisi è costantemente ripetuta nel tempo alla luce dei progressi tecnologici, dei mutamenti normativi e del riscontro ottenuto dai controlli sulle misure già adottate.

### **Art. 3**

(Definizioni di riferimento)

1. Ai fini del presente documento, si fa riferimento alle definizioni contenute nel Titolo I, art. 4 (Definizioni) del Codice.
2. Per finalità istituzionali, ai sensi dell'art. 18 del Codice, si intendono:
  - a) le funzioni attribuite alla Giunta della Regione Emilia-Romagna dalla legge e/o della normativa comunitaria;
  - b) le funzioni attribuite dallo Statuto regionale;
  - c) le funzioni attribuite dai regolamenti;
  - d) le funzioni attribuite per mezzo di convenzioni, accordi, intese e mediante gli strumenti di programmazione negoziata previsti dalla normativa vigente;
  - e) le attività collegate all'accesso e all'erogazione dei servizi resi dalla Giunta della Regione Emilia-Romagna;
  - f) le attività necessarie per soddisfare finalità di rilevante interesse pubblico;
  - g) le attività di studio, ricerca e/o contabili-amministrative;
  - h) le attività volte a soddisfare esigenze informative, operative e gestionali per il migliore svolgimento dei compiti istituzionali e del mandato politico-istituzionale.

### **Art. 4**

(Ambito di applicazione)

1. Le linee guida disciplinano l'attività dei dipendenti appartenenti all'organico della Giunta della Regione Emilia-Romagna che effettuano trattamenti di dati personali nonché di tutti coloro che a vario titolo li effettuano in nome e/o per conto della Giunta medesima, siano essi responsabili o incaricati.
2. Le linee guida si applicano sia ai trattamenti effettuati con l'ausilio di strumenti elettronici sia ai trattamenti effettuati senza l'ausilio di strumenti elettronici.

### **Art. 5**

(Tutela del patrimonio informativo)

1. La tutela del patrimonio delle informazioni riveste importanza strategica per la Giunta della Regione Emilia-Romagna, oltre che essere soggetta a precisi vincoli di legge imposti dal Codice.

2. La sicurezza delle informazioni è definita come la salvaguardia di *riservatezza*, *integrità* e *disponibilità* delle stesse.

In particolare:

- a) tutelare la *riservatezza* significa assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati ad avervi accesso;
- b) tutelare l'*integrità* significa salvaguardare l'accuratezza e completezza delle informazioni e del loro trattamento;
- c) tutelare la *disponibilità* significa assicurare che gli utenti autorizzati abbiano accesso, quando richiesto, alle informazioni e ai beni ad esse associati.

3. Il comportamento dei destinatari di queste linee guida deve essere improntato alla tutela della sicurezza delle informazioni.

## **Art. 6**

(Sensibilizzazione)

1. La sicurezza di un sistema è costituita da tecnologie, procedure e comportamenti di tutti gli utenti del sistema stesso. Ciò rende fondamentale la sensibilizzazione di tutti coloro che effettuano trattamenti di dati personali circa i rischi incombenti sui dati e circa il corretto utilizzo dei relativi strumenti di protezione disponibili. Tale sensibilizzazione è fondamentale per assicurare la sicurezza dei sistemi e delle reti d'informazione.

2. I sistemi e le reti d'informazione sono sottoposti a rischi interni ed esterni, quindi è necessario che tutti sappiano e siano consapevoli che, a causa dell'interconnettività e dell'interdipendenza tra sistemi, falle in materia di sicurezza su un componente del sistema possono propagare i loro effetti fino ad incidere gravemente sull'integrità dei sistemi, delle reti, delle banche dati, degli archivi e arrecare danni ad altri.

3. Comportamenti non partecipi, disinformati o indifferenti, possono ostacolare gravemente la tutela del patrimonio informativo e ledere il rapporto di fiducia che deve necessariamente intercorrere tra l'amministrazione regionale e la società civile.

## **Art. 7**

(Responsabilità)

1. Tutti coloro che effettuano trattamenti di dati personali devono essere consapevoli del fatto che la loro azione o inazione può causare danni ad altri o ledere diritti altrui.

2. La società dell'informazione dipende da sistemi e da reti d'informazione locali e globali interconnessi; per questo motivo tutti coloro che effettuano trattamenti di dati personali, devono essere consapevoli della propria responsabilità rispetto alla

sicurezza del sistema nel suo complesso, in funzione del proprio ruolo e devono adeguare le proprie pratiche, misure e procedure affinché siano coerenti con queste linee guida e con il sistema di protezione delle informazioni adottato dalla Giunta regionale.

3. Coloro che gestiscono, sviluppano, progettano e forniscono prodotti e servizi nell'ambito dei sistemi informativi, devono agire in modo da garantire la sicurezza dei sistemi e delle reti, tutelare la riservatezza dei dati personali e diffondere informazioni utili per assicurare l'adozione di idonee pratiche di sicurezza.

4. Un comportamento responsabile è quindi indispensabile e tutti, per il proprio ambito di competenza, devono adoperarsi per elaborare e adottare pratiche esemplari e incoraggiare comportamenti che tengano conto degli imperativi di sicurezza e di tutela dei diritti altrui.

### **Art. 8**

(Risposta agli incidenti di sicurezza)

1. I soggetti che effettuano il trattamento devono operare tempestivamente e in uno spirito di collaborazione per prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile.

2. A causa dell'interconnettività dei sistemi e delle reti d'informazione, gli impatti causati da un incidente di sicurezza si diffondono rapidamente ed in modo molto esteso; è necessario quindi che i soggetti che effettuano il trattamento, in funzione del proprio ruolo, reagiscano agli incidenti di sicurezza con prontezza e con spirito di collaborazione. In particolare tutti devono contribuire per prevenire gli incidenti di sicurezza e garantire una risposta adeguata.

### **Art. 9**

(Diritto di accesso dell'interessato ai propri dati personali)

1. I soggetti che effettuano il trattamento dei dati personali devono operare tempestivamente e in uno spirito di collaborazione per garantire all'interessato un accesso agevole, certo e semplificato ai propri dati personali e per favorire la corretta gestione delle istanze dell'interessato per un riscontro chiaro ed esauriente nel minor tempo possibile.

2. Il diritto dell'interessato di tutelare i propri dati personali e l'imposizione di regole di comportamento a tutti coloro che effettuano operazioni sui medesimi, danno concreta attuazione ai principi di eguaglianza e dignità sociale della persona.

3. Le regole tecniche in materia di diritto di accesso dell'interessato ai propri dati personali sono definite ai sensi dell'articolo 16 delle presenti linee guida.

## Art. 10

(Trasparenza amministrativa e diritto d'accesso ai documenti amministrativi)

1. La tutela della privacy e dei diritti dell'interessato, così come la sicurezza dei sistemi e delle reti d'informazione, devono essere compatibili con i valori fondamentali di una società democratica e, in particolare, con il principio di trasparenza dell'attività amministrativa.
2. La Regione Emilia-Romagna, al fine di agevolare l'attuazione del principio di trasparenza, provvede alla diffusione, oltre che sul Bollettino Ufficiale, tramite le proprie reti telematiche, dell'elenco e dei testi dei propri atti amministrativi di natura generale.
3. Gli atti amministrativi devono essere redatti dai destinatari di queste linee guida riportando direttamente nell'oggetto e nel testo soltanto i dati personali strettamente necessari alla finalità dell'atto.
4. In particolare gli atti che devono essere pubblicati sul Bollettino Ufficiale della Regione, o sottoposti ad altre forme di pubblicità previste da legge o regolamento, non devono riportare nell'oggetto e nel testo dati sensibili e/o giudiziari se non nei casi previsti da espressa disposizione di legge. Non devono in nessun caso essere riportati direttamente dati idonei a rivelare lo stato di salute di persone identificate o identificabili. Nel caso in cui i suddetti dati siano indispensabili per la finalità dell'atto, nella pubblicizzazione devono essere adottate opportune misure che evitino l'associazione, anche indiretta, all'interessato, ad esempio tramite l'impiego di diciture generiche o codici alfanumerici.
5. Quanto previsto dal precedente capoverso deve essere applicato anche nel caso di diffusione attraverso le bacheche, comprese quelle telematiche.
6. La Giunta della Regione Emilia-Romagna può pubblicare sul proprio sito internet, al fine di agevolare la comunicazione con il pubblico, i numeri telefonici e l'indirizzo e-mail istituzionale delle proprie strutture o dei dipendenti che operano presso le stesse. Essi possono essere utilizzati soltanto per fini inerenti alle attività istituzionali della Giunta della Regione Emilia-Romagna. In particolare, non possono essere utilizzati per finalità pubblicitarie o commerciali. Di questa limitazione all'utilizzo da parte dei terzi è riportato avviso nel sito web della Giunta della Regione Emilia-Romagna.
7. In materia di diritto di accesso ai documenti amministrativi, il principio di trasparenza può prevalere sulla tutela della riservatezza, consentendo al legittimo titolare del diritto di accedere anche ai documenti contenenti dati personali di terzi la cui conoscenza è necessaria per la cura o la difesa dei suoi interessi giuridici.
8. Nel caso di istanza d'accesso a documenti amministrativi contenenti dati sensibili e giudiziari, l'esercizio del diritto è concesso tuttavia nei limiti strettamente indispensabili. Peraltro, quando i documenti contengono dati idonei a rivelare lo stato di salute e la vita sessuale di terzi, l'accesso è consentito soltanto se strumentale alla tutela di un diritto della personalità o altro diritto o libertà fondamentale e inviolabile o, comunque, a tutela di una situazione giuridica di

rango almeno pari ai diritti dell'interessato.

### **Art. 11**

(Uso delle strumentazioni informatiche)

1. Le strumentazioni informatiche che la Giunta della Regione Emilia-Romagna mette a disposizione devono essere utilizzate in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.
2. Con specifico riferimento agli strumenti informatici e telematici, alla posta elettronica e a Internet, i destinatari delle presenti linee guida sono tenuti in particolare a:
  - a) utilizzare tali beni per motivi non attinenti all'attività lavorativa soltanto in casi di urgenza e comunque non in modo ripetuto o per periodi di tempo prolungati;
  - b) utilizzare la posta elettronica e Internet nel rispetto del principio di riservatezza, per le specifiche finalità della propria attività e rispettando le esigenze di funzionalità della rete e quelle di semplificazione dei processi lavorativi;
  - c) non appesantire il traffico della rete con operazioni particolarmente lunghe e complesse quando ciò non sia necessario allo svolgimento dell'attività lavorativa.
3. Le regole tecniche in materia di utilizzo delle strumentazioni informatiche sono definite ai sensi dell'articolo 16 delle presenti linee guida.

### **Art. 12**

(Segnalazione delle violazioni)

1. Le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste per un determinato trattamento, devono essere tempestivamente segnalate secondo le modalità e le regole tecniche definite ai sensi dell'articolo 16 delle presenti linee guida.

### **Art. 13**

(Controlli di sicurezza)

1. La Giunta della Regione Emilia-Romagna si riserva la facoltà di effettuare i controlli ritenuti opportuni per la verifica della corretta applicazione e dell'efficienza delle misure di sicurezza adottate per la protezione dei dati personali.
2. Tali controlli possono essere effettuati esclusivamente da personale debitamente autorizzato secondo modalità dipendenti dal valore dei dati trattati e dai rischi di sicurezza che incombono su di essi.
3. In ogni caso, le modalità dei controlli devono essere preventivamente

comunicate ed illustrate a chi effettua trattamenti di dati personali nei modi previsti dall'art. 16.

#### **Art. 14**

(Sanzioni)

1. La violazione di comportamenti prescritti nelle presenti linee guida può comportare l'applicazione di una sanzione disciplinare se la fattispecie integra gli estremi di una infrazione prevista dai Contratti Collettivi o determinare una responsabilità dirigenziale, – ferma restando anche una possibile responsabilità penale, civile o amministrativa-contabile.

#### **Art. 15**

(Registro informatico dei trattamenti dei dati personali ed Elenco dei responsabili del trattamento)

1. Si istituisce il Registro informatico dei trattamenti dei dati personali per censire i trattamenti effettuati nell'ambito delle strutture afferenti alla Giunta regionale e le relative banche dati. Tale Registro costituisce il supporto necessario alla redazione e all'aggiornamento annuale del Documento Programmatico per la Sicurezza. È fatto obbligo ai Responsabili del trattamento, di cui al paragrafo 3 della Deliberazione n. 960 del 27/06/2005, di provvedere all'aggiornamento del Registro con cadenza almeno annuale. Tali Responsabili possono individuare uno o più addetti incaricati del censimento e dell'aggiornamento dei trattamenti di competenza.

2. La supervisione del Registro e degli aggiornamenti effettuati, nonché l'estrazione dei dati in forma omogenea per il loro utilizzo nell'aggiornamento annuale del Documento Programmatico per la Sicurezza compete al Responsabile della Sicurezza.

3. L'Elenco dei responsabili interni ed esterni, al fine di renderlo conoscibile in modo agevole e chiaro agli interessati, come stabilito dal Codice, è pubblicato sul sito ufficiale regionale a cura del Coordinatore del diritto di accesso dell'interessato ai propri dati personali.

4. L'Elenco deve essere tempestivamente aggiornato. Al fine di consentire un puntuale aggiornamento, gli atti e i documenti di nomina e di individuazione dei Responsabili interni ed esterni devono essere resi noti al Coordinatore del diritto di accesso dell'interessato ai propri dati personali.

5. In sede di aggiornamento del Registro informatico dei trattamenti, il Coordinatore del diritto di accesso dell'interessato ai propri dati personali, in accordo con il Responsabile della Sicurezza, verifica la corrispondenza tra l'Elenco ed il Registro.

## **Art. 16**

(Disciplinari tecnici)

1. L'applicazione pratica dei principi contenuti in queste linee guida è definita attraverso appositi disciplinari tecnici secondo quanto stabilito dal paragrafo 3 della Deliberazione n. 960 del 27/06/2005.

2. I disciplinari tecnici contengono specifiche indicazioni comportamentali e/o procedurali rivolte principalmente ai responsabili e agli incaricati dei trattamenti di dati personali nonché agli altri soggetti che, nello svolgimento della propria attività, possono ostacolare il raggiungimento delle finalità di cui all'Art.1 delle presenti linee guida.

- - - - -