

INDICE

| | |
|---|----|
| Introduzione | 5 |
| Parte I ^ | |
| 1. Finalità e principi generali del D.lgs. 196/2003 | 8 |
| 2. Definizioni | 10 |
| 2.1. Dati | 10 |
| 2.2. Operazioni | 11 |
| 2.3. Soggetti | 12 |
| 2.4. Misure di sicurezza | 13 |
| Parte II ^ | |
| 3. Ambito di applicazione | 16 |
| 4. Modalità e disposizioni organizzative della Regione Toscana | 16 |
| 4.1. Ufficio Privacy Regionale | 16 |
| 4.2. Soggetti che trattano i dati personali | 18 |
| 4.2.1. Titolare | 18 |
| 4.2.2. Responsabile | 20 |
| 4.2.2.1. Funzioni dei responsabili dei trattamenti dei dati | 22 |
| 4.2.3. Incaricati | 25 |
| 5. Disposizioni generali per il trattamento dei dati personali | 26 |
| 5.1. Elenco regionale dei trattamenti di dati personali | 26 |
| 5.2. Il trattamento dei dati personali | 27 |
| 5.3. Comunicazione e diffusione dei dati personali comuni | 29 |
| 5.4. Diffusione di dati personali comuni tramite pubblicazione sul B.U.R.T. | 30 |

| | | |
|----------|--|----|
| 5.5. | Trattamento di dati personali sensibili e giudiziari | 31 |
| 5.6. | Trattamento dei dati personali sensibili | 32 |
| 5.6.1. | Adeguamento dell'ordinamento regionale | 32 |
| 5.6.2. | Esclusione del consenso | 33 |
| 5.6.3. | Dati idonei a rivelare lo stato di salute | 33 |
| 5.6.3.1. | Cifratura o separazione degli altri dati personali dell'interessato | 34 |
| 5.6.4. | Diffusione dei dati personali sensibili tramite pubblicazione sul B.U.R.T. | 36 |
| 5.7. | Trattamento dei dati personali giudiziari | 36 |
| 5.7.1. | Diffusione dei dati giudiziari tramite pubblicazione sul B.U.R.T. | 38 |
| 5.8. | Trattamenti di dati personali per scopi statistici, storici e di ricerca scientifica | 39 |
| 5.8.1. | Trattamento di dati personali per scopi storici | 39 |
| 5.8.2. | Trattamento di dati raccolti per scopi statistici e di ricerca scientifica | 40 |
| 5.8.2.1. | Codici di deontologia e di buona condotta | 40 |
| 5.8.2.2. | Trattamento di dati personali per fini statistici nell'ambito del Programma Statistico Regionale e Nazionale | 41 |
| 5.8.2.3. | Trattamento di dati personali per fini statistici e di ricerca | 42 |

| | | |
|-----------|---|-----------|
| 5.8.2.4. | Ricerca scientifica in ambito sanitario | 43 |
| 6. | Rapporti con l’Autorità Garante | 43 |
| 7. | Adempimenti | |
| 7.1. | Notificazione al garante per la protezione dei dati personali | 44 |
| 7.2. | Informativa agli interessati | 45 |
| 7.3. | Diritti dell'interessato | 48 |
| 7.3.1. | Esercizio dei diritti dell'interessato | 49 |
| 8. | Rapporti tra la normativa sulla privacy e il diritto di accesso. | |
| 8.1. | Accesso agli atti amministrativi | 50 |
| 8.1.1. | Diritto di accesso dei consiglieri regionali | 51 |
| 9. | Misure di Sicurezza | 52 |
| 9.1. | Sicurezza degli archivi cartacei | 54 |
| 9.1.1. | Archivi di lavoro | 54 |
| 9.1.2. | Archivio dei fascicoli del personale | 55 |
| 9.1.3. | Archivio storico (Osmannoro) | 55 |
| 9.2. | Accesso ai dati particolari | 56 |
| 9.3. | Adempimenti relativi ai fornitori che possono venire a conoscenza di dati personali | 56 |
| 9.4. | Documento Programmatico sulla Sicurezza | 58 |

| | | |
|------------------|--|----|
| Allegati: | | 59 |
| Allegato n.1 | “Misure di sicurezza relative al trattamento di dati personali, ruoli e funzioni nella struttura organizzativa del Titolare Giunta Regionale.” | 60 |
| Allegato n. 2 | “Linee guida per gli utenti in merito alle Misure Minime di Sicurezza” | 64 |
| Allegato n. 3 | Modulistica/Fac-Simile | 71 |
| | a) Informativa ex art. 13 D.lgs. 196/03 | |
| | b) Ordine di servizio per la nomina degli incaricati | |
| | c) Nomina del responsabile esterno | |
| | d) Modello per l'esercizio dei diritti | |
| | e) Accesso al registro dei trattamenti tenuto dal Garante per la protezione dei dati personali | |

**DIRETTIVA PER L'ATTUAZIONE DEL DECRETO
LEGISLATIVO 30 GIUGNO 2003, N. 196,
"CODICE IN MATERIA DI PROTEZIONE DEI DATI
PERSONALI"..**

I INTRODUZIONE

L'evoluzione del concetto di riservatezza dell'individuo, nel percorso seguito fino ad oggi per affermarsi nel nostro ordinamento, si è incentrata più recentemente su un'idea di centralità della persona nella gestione dei dati che la riguardano.

La necessità per la Pubblica Amministrazione di acquisire le informazioni indispensabili per lo svolgimento delle proprie attività istituzionali, ma soprattutto il progressivo mutamento della società verso modelli di comunicazione sempre più integrati ed interconnessi (la c.d. "società dell'informazione"), 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;

La Legge 675/1996, dando attuazione alla Direttiva europea 95/46/CE, ha disciplinato in modo più preciso questa materia, costruendo un impianto che tende a mettere l'interessato in condizione di seguire i propri dati personali e di intervenire per limitarne l'uso e, soprattutto, l'abuso. In seguito, nel 2003 è stato emanato il Decreto legislativo 30 giugno, n. 196 contenente il Codice in materia di protezione dei dati personali, testo unico pubblicato nel supplemento ordinario n. 123 alla Gazzetta Ufficiale n. 174 del 29 luglio 2003 ed entrato in vigore dall'1 gennaio 2004.

Con tale provvedimento lo Stato, in sintonia con le Direttive Europee, ha provveduto a raccogliere e coordinare i decreti

Il Codice in materia di protezione dei dati personali: il nuovo testo unico

legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni, e a recepire la "giurisprudenza" del Garante.

Il testo unico, di rango legislativo, nel rispetto del principio di semplificazione, ha come primo obiettivo quello di dar corso ad una sistemazione della materia al fine, anche, di renderla più facilmente comprensibile. Non mancano però numerose modifiche e integrazioni innovative, volte, fra l'altro, a completare o perfezionare il recepimento della Direttiva 95/46/CE e ad aggiornare le norme vigenti in materia di protezione della vita privata nel mondo delle telecomunicazioni di cui alla Direttiva n. 2002/58/CE.

Il D.Lgs. n. 196/2003 introduce significative novità rispetto alla legge n. 675/1996 anche per quel che concerne il profilo sanzionatorio.

Vengono infatti riconosciute responsabilità civili e penali e, proprio per questo, sono ulteriormente precisate una serie di misure minime a cui tutti i soggetti titolari di trattamento devono obbligatoriamente sottostare per evitare sanzioni penali e risarcimento dei danni provocati.

Il trattamento dei dati personali è infatti equiparato ad attività pericolosa (art. 15 c. 1), ai sensi dell'art. 2050 del codice civile. In base a questa norma il titolare sarà tenuto a risarcire i danni, a meno che non provi di aver adottato le misure "idonee" (non le "minime") per evitare il danno. La novità è nel secondo comma dell'art. 15, secondo il quale il danno non patrimoniale è risarcibile anche in caso di violazione delle norme attinenti alle modalità del trattamento comprendenti anche le regole sulla conservazione.

Di conseguenza, chi trattando dati personali provoca danni ad altri è tenuto al risarcimento.

Il Codice, oltre ad eventuali sanzioni amministrative che possono arrivare fino a 125.000 Euro, prevede specifici reati penali con pene fino a tre anni di reclusione.

A chi si rivolge la Direttiva

La presente Direttiva fornisce indirizzi e modalità organizzative all'interno della Regione Toscana.

Essa costituisce anche un modello di riferimento per gli enti, le aziende e le agenzie regionali e i soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e

controllo, contribuendo così a definire il “percorso privacy nella comunità regionale toscana”.

Il livello di recepimento della Direttiva da parte dei soggetti del Sistema degli enti regionali ovviamente sarà congruente con i diversi relativi livelli di autonomia organizzativa e amministrativa.

La presente Direttiva costituisce uno strumento operativo per i vari soggetti che assumono ruoli di responsabilità nel trattamento dei dati personali. In particolare mira a fornire a Dirigenti e operatori, oltre alle informazioni sui principi fondamentali della legge, indicazioni pratiche in ordine alle varie misure (organizzative, procedurali, tecniche e logistiche) da applicare per garantire un buon livello di sicurezza dei dati personali trattati per il perseguimento delle finalità istituzionali.

| |
|-----------------------------|
| Finalità della Direttiva |
|-----------------------------|

Inoltre, tramite l'individuazione puntuale dei compiti e degli adempimenti spettanti ai vari soggetti coinvolti nella gestione dei dati personali, compresi i collaboratori esterni, la Direttiva definisce anche l'estensione ed i limiti delle loro responsabilità.

La Direttiva si articola in tre sezioni:

- una parte introduttiva (Parte I), propedeutica alla conoscenza delle finalità e dei principi generali del Codice;
- una Parte II, di carattere operativo, specificatamente dedicata agli adempimenti previsti dal Codice, ivi comprese le misure di sicurezza, che i vari soggetti della Regione Toscana sono tenuti a rispettare;
- una Parte III dedicata alla modulistica occorrente per adempiere agli obblighi richiamati nel presente documento.

Per facilitarne la reperibilità, il testo del presente documento è disponibile in Intranet, all'indirizzo:

<https://www.regione.toscana.it/intranet>,

selezionando la voce “Privacy”, e sul sito web della Regione Toscana.

PARTE I ^

1. FINALITÀ E PRINCIPI GENERALI DEL D.LGS. 196/2003

Finalità e principi del Codice in materia di protezione dei dati personali

Il Codice della privacy, in aderenza alla disciplina dell'Unione Europea, intende garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Disciplina in particolare la protezione di diritti della persona riconosciuti come inviolabili e fondamentali dall'articolo 2 della Costituzione, quali:

- **il diritto alla riservatezza:** diritto di ognuno a mantenere la propria vita privata libera da ingerenze esterne;
- **il diritto all'identità personale:** diritto di ognuno ad utilizzare in esclusiva il proprio nome e altri elementi identificativi della propria persona.

Principio di necessità

Una novità introdotta è il "**principio di necessità**" del trattamento dei dati (art. 3 del Codice). Esso afferma che i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'uso di dati personali/dati identificativi. Così il loro trattamento è escluso quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Principi di pertinenza e non eccedenza

Il nuovo principio introdotto integra e completa il principio di **pertinenza e non eccedenza** dei dati trattati, in base ai quali i dati possono essere trattati solo se funzionali al raggiungimento degli scopi legittimi perseguiti, completi e non eccessivi rispetto agli scopi stessi.

Il Codice disciplina il **trattamento di dati personali**, anche detenuti all'estero, effettuato da chiunque si trovi in territorio nazionale. Si applica anche al trattamento effettuato da parte di soggetti eventualmente extra-UE che utilizzino - per il trattamento - strumenti situati in Italia (anche diversi da

quelli elettronici), salvo che si tratti di un “mero transito di dati nell’UE”.

I soggetti pubblici – ad eccezione degli enti pubblici economici (il cui regime è equiparato a quello dei privati) – trattano dati personali solo quando ciò è necessario per svolgere le loro funzioni istituzionali, nei limiti stabiliti dal Codice Privacy, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti, ai sensi dell’art.18 del Codice.

| |
|--|
| Il trattamento è consentito solo per lo svolgimento delle funzioni istituzionali e nei limiti dettati da leggi e regolamenti |
|--|

Anche quando l’amministrazione persegue finalità istituzionali mediante gli strumenti del diritto privato (disciplina del rapporto di lavoro, attività contrattuale, ecc.), ai fini della normativa sulla protezione dei dati personali essa è comunque da considerarsi soggetto pubblico, avendo rilevanza l’aspetto soggettivo della stessa e non la natura dei rapporti gestiti.

Questo aspetto determina un diverso regime fra soggetti privati e pubblici.

I soggetti pubblici non devono richiedere il consenso dell’interessato, tranne che, in via eccezionale, per il trattamento dei dati effettuato dagli organismi sanitari pubblici per perseguire una finalità di tutela della salute o dell’incolumità fisica dell’interessato.

In presenza dei presupposti giuridici, la pubblica amministrazione può quindi legittimamente trattare i dati personali, **senza acquisire il consenso** dell’interessato.

Al contrario, l’acquisizione del consenso dell’interessato **non legittima** l’amministrazione a trattare i dati per finalità diverse da quelle istituzionali o a effettuare operazioni non consentite da leggi o regolamenti.

2. DEFINIZIONI

La terminologia adottata nella presente Direttiva, è conforme a quanto previsto dall'art. 4 del D.Lgs n. 196/2003, ed è qui raggruppata per *dati, operazioni, soggetti e misure di sicurezza*, per consentirne una più agevole individuazione.

2.1. *Dati*

Dato personale: qualunque informazione relativa a un soggetto identificato o identificabile

Dati identificativi

Identificabilità

a) Il **"dato personale"**, secondo la sua definizione generale, è qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, che può essere identificato in modo diretto o indiretto.

b) All'interno di questa definizione più generale si specificano ulteriori tipologie di dati: i **"dati identificativi"**, che sono i dati immediatamente associati ad una persona determinata.

Un soggetto si intende identificabile quando è possibile associare le informazioni ai dati identificativi del soggetto, attraverso l'impiego di mezzi ragionevoli

Il Codice inoltre individua i **dati sensibili, i dati giudiziari, gli altri dati particolari, i dati cosiddetti comuni.**

Questa classificazione è stabilita in funzione del diverso livello di riservatezza intrinseco alle varie tipologie di dati, delle diverse precauzioni che la legge richiede per il loro utilizzo, per la loro custodia e per il loro trattamento e della oggettiva diversa pericolosità per l'individuo derivante da un eventuale illecito trattamento.

Dati sensibili

c) I **"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.

La definizione di dato sensibile è esclusiva: sono considerati tali solo i dati specificamente indicati, indipendentemente dal carattere di riservatezza o di particolare rilevanza che un

individuo, o il senso comune, può attribuire ad altre tipologie di dati (ad esempio: coordinate bancarie, reddito, etc.)

d) I **“dati giudiziari”** sono i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o a rivelare la qualità di imputato o di indagato ai sensi del codice di procedura penale.

Dati giudiziari

e) Un'ulteriore categoria è quella prevista **dall'articolo 17** del Codice, intermedia tra dati sensibili e comuni, il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Il loro trattamento è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato ove prescritti dal Garante.

Altri dati particolari

f) I dati che, per semplicità, si è soliti definire **“dati comuni”** sono tutti i restanti dati personali, non compresi nelle precedenti categorie (es.: dati anagrafici, coordinate bancarie, codice fiscale).

Dati personali comuni

2.2. Operazioni

a) Per **“trattamento”** si deve intendere qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, 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.

Trattamento: qualunque operazione, tra quelle indicate dal Codice, effettuata sui dati

Nell'ambito delle varie fasi del trattamento, particolare attenzione viene riservata dalla legge a quelle relative alla comunicazione e alla diffusione, a cui viene attribuito il seguente significato.

Comunicazione e diffusione: portare i dati personali a conoscenza di uno o più soggetti determinati o indeterminati

b) Per **“comunicazione”**: si intende 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.

- c) Per "**diffusione**": si intende il dare conoscenza dei dati personali **a soggetti indeterminati**, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Tale conoscenza si intende ovviamente riferita ai dati personali e non ai risultati di eventuali elaborazioni, che non ricadono nel campo di applicazione della legge.

2.3. *Soggetti*

Soggetti che trattano i dati.

Il trattamento dei dati è ammesso solo da parte del Titolare dei dati, dei Responsabili del trattamento dei dati e degli incaricati, con l'attribuzione di compiti e responsabilità a questi soggetti, in relazione al ruolo da essi svolto nell'ambito del trattamento.

Il Titolare è la persona fisica o giuridica che decide

- a) Il "**Titolare**" è il soggetto (persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo) investito del potere decisionale circa le attività di trattamento dei dati personali, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il Responsabile è preposto dal titolare al trattamento dei dati

- b) Il "**Responsabile del trattamento dei dati personali**" è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Il Responsabile viene designato dal titolare tra coloro che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

La designazione del Responsabile del trattamento è facoltativa.

- c) Gli "**Incaricati**" del trattamento dei dati personali sono i soggetti che effettuano materialmente le operazioni di trattamento.

Incaricati e loro individuazione

Possono essere individuati incaricati solo le persone fisiche.

Essi sono nominati per iscritto dal Responsabile, che individua puntualmente l'ambito di trattamento consentito e fornisce loro le istruzioni.

Si considera individuazione degli incaricati anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima (art. 30 del Codice).

L'atto di nomina si configura come autorizzazione al trattamento dei dati e costituisce l'unico presupposto di liceità per l'uso dei dati stessi.

Gli incaricati operano sotto la diretta autorità del titolare o del Responsabile e devono effettuare i trattamenti dei dati attenendosi alle istruzioni ricevute e nel rispetto delle indicazioni relative alle norme di sicurezza.

Gli incaricati del trattamento sono formati in modo tale da permettere loro di acquisire conoscenza sul corretto uso dei dati oltre a renderli edotti sui principi fondamentali del Codice.

La formazione per i neo-assunti è programmata sin dalla loro entrata in servizio, secondo quanto previsto dalla legge.

- d) "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
- e) "**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2.4. *Misure di sicurezza*

Le misure di sicurezza sono articolate in due gruppi correlati. Il primo inserito nel corpo del Codice agli articoli 31, 32, 33, 34, 35, 36; il secondo riportato in allegato nel "*Disciplinare tecnico*" o "*Allegato B*", composto da 29 dettagliate prescrizioni.

Misure di sicurezza

Misure minime di sicurezza

Misure idonee

- a) Per "**misure minime**" si intende 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 dall'art. 31 del D.Lgs. 196/2003.
- b) Le "**misure idonee**" sono le misure volte a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti.

Rispetto alle disposizioni contenute nel D.P.R. n. 318/99, il sistema delle misure minime di sicurezza viene semplificato e aggiornato sulla base dell'esperienza applicativa acquisita e dell'evoluzione tecnologica.

In particolare, ai fini dell'applicazione delle misure minime richieste, si conferma la distinzione fra trattamenti effettuati con strumenti elettronici e trattamenti "cartacei", senza che vi sia l'ulteriore distinzione tra trattamenti effettuati con elaboratori accessibili da altri elaboratori o terminali e trattamenti con elaboratori accessibili in rete.

- c) "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- d) "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- e) "**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;
- f) "**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;
- g) "**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;

h) "**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.

Ai fini della presente Direttiva si intende, inoltre, per:

- a) "**scopi storici**", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- b) "**scopi statistici**", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- c) "**scopi scientifici**", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.



PARTE II ^

3. AMBITO DI APPLICAZIONE

La presente Direttiva disciplina il trattamento di dati personali effettuato dalla Regione Toscana in applicazione dei principi di cui al D.Lgs. 196 del 30 giugno 2003 (di seguito denominato "codice" o "testo unico") in materia di protezione dei dati personali.

La Regione, secondo quanto previsto dall'art. 18 del Codice, provvede al trattamento dei dati personali per lo svolgimento dei propri fini istituzionali, nei limiti stabiliti dallo Statuto, dalle leggi e dai regolamenti e in ogni caso nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con riferimento particolare alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

4. MODALITÀ E DISPOSIZIONI ORGANIZZATIVE DELLA REGIONE TOSCANA

4.1. UFFICIO PRIVACY REGIONALE

| |
|---|
| Ruolo e compiti dell' Ufficio Privacy Regionale |
|---|

L'attuazione delle disposizioni del Testo Unico richiede di assicurare l'omogeneità delle soluzioni organizzative, procedurali e di funzionamento dei servizi; di assicurare la necessaria unitarietà e coerenza metodologica nell'impostazione e conseguente programmazione operativa degli adempimenti connessi alla protezione dei dati personali in riferimento ai nuovi assetti organizzativo-gestionali delle strutture regionali.

Pertanto allo scopo di garantire continuità e unitarietà di indirizzo e di presidiare con modalità coordinate e unitarie la gestione delle attività connesse all'attuazione della normativa privacy nella Regione Toscana, il Settore Sistema Statistico Regionale, al quale è stata attribuita la responsabilità e la competenza in materia di privacy, avvalendosi della Posizione Organizzativa assegnata e denominata "Ufficio Privacy Regionale", svolge le funzioni di:

- a) fornire indirizzi e linee guida alle strutture regionali e agli enti regionali al fine di una corretta attuazione della normativa in materia di privacy
- b) promuovere e realizzare iniziative per la diffusione della cultura della privacy nella regione Toscana
- c) curare i rapporti con l'ufficio del Garante per gli aspetti tecnico-operativi connessi all'attuazione della normativa in ambito regionale, richieste di chiarimenti, richieste di pareri formali, etc., a supporto delle Direzioni generali, allo scopo di evitare frammentazioni
- d) curare, per conto del titolare Regione Toscana – Giunta Regionale, gli adempimenti previsti d'obbligo dal D.Lgs. 196/2003 e cioè: Comunicazione e Notificazione al Garante, Regolamento dei dati sensibili e giudiziari previsto dagli artt. 20-21 e relativo aggiornamento, Documento programmatico per la sicurezza e relativo monitoraggio
- e) riferire dell'avvenuta redazione o aggiornamento del Documento programmatico per la sicurezza alla Direzione generale Bilancio e Finanze perché ne dia segnalazione nella relazione accompagnatrice del bilancio di esercizio
- f) assicurare attività di consulenza e supporto tecnico alle Direzioni generali, agli uffici regionali, agli Enti e alle Agenzie regionali ed inoltre di consulenza ad altri soggetti della pubblica amministrazione (per le materie oggetto di delega da parte della Regione) sui contenuti della normativa e in relazione agli adempimenti
- g) collaborare alla stesura di proposte di regolamento regionale su tematiche che implicano il trattamento di dati personali
- h) garantire la supervisione di iniziative e/o progetti che implicano l'utilizzo di dati personali
- i) operare per la composizione delle controversie sui dati personali, e più in generale in tema di riservatezza
- j) definire, in collaborazione con il Settore "Organizzazione, Formazione, Sviluppo Organizzativo, Reclutamento, il programma di formazione a carattere permanente sul tema della protezione dei dati personali per il personale regionale, assicurando l'obbligo formativo previsto dal Codice

- k) coordinare il gruppo dei Referenti del "Sistema Privacy" – (RSP) – individuati nelle singole Direzioni generali, costituito in attuazione della Decisione della Giunta regionale n. 5 del 23-01-2006, per l'attuazione della normativa in materia di protezione di dati personali nell'intera struttura regionale
- l) vigilare sull'osservanza della presente Direttiva regionale sulla privacy fornendo la necessaria consulenza in ordine all'adeguamento dei percorsi e delle procedure regionali per quanto attiene l'aspetto della riservatezza dei dati e monitorare l'attuazione del Documento Programmatico della Sicurezza
- m) redigere la relazione di sintesi sullo stato di applicazione della normativa per la Giunta Regionale, anche sulla base delle relazioni ricevute da ciascun direttore generale
- n) coordinare l'aggiornamento dell'Archivio regionale dei trattamenti dei dati personali

Nell'esercizio delle competenze di cui ai punti precedenti deve essere garantito all'Ufficio Privacy Regionale l'apporto di tutte le articolazioni organizzative dell'amministrazione regionale e la collaborazione dei referenti del "Sistema Privacy".

4.2. SOGGETTI CHE TRATTANO I DATI PERSONALI

L'applicazione delle norme del Codice comporta l'attribuzione di compiti e responsabilità ai soggetti da esso previsti.

4.2.1. TITOLARE

Titolare è la Regione Toscana – Giunta Regionale

Con deliberazione della Giunta Regionale n. 208 del 9.3.1998 è stato individuato l'ente "**Regione Toscana - Giunta Regionale**" quale titolare dei trattamenti di dati personali effettuati nei dipartimenti (oggi Direzioni generali) e uffici della Regione Toscana, con esclusione dell'ambito di competenza del Consiglio regionale.

Compiti del Titolare

Il Titolare, con l'ausilio dell'Ufficio Privacy Regionale, provvede ad assolvere agli obblighi previsti dalla normativa nazionale in materia di riservatezza dei dati personali e in particolare:

- a) nomina i Responsabili del trattamento, impartendo loro le necessarie istruzioni
- b) effettua la notificazione al Garante, ai sensi dell'art. 37 del D.Lgs. n. 196/2003
- c) adotta il Regolamento dei dati sensibili e giudiziari ai sensi degli artt. 20 e 21 del Codice
- d) richiede al Garante, qualora necessaria, l'autorizzazione al trattamento dei dati sensibili
- e) effettua la comunicazione al Garante, necessaria nel caso si debbano comunicare dati personali comuni a soggetti pubblici in assenza di disposizione di legge che lo preveda espressamente.
- f) redige il Documento Programmatico per la sicurezza
- g) adotta le misure di sicurezza

I Direttori generali del Centro Direzionale e dell'Avvocatura provvedono, **per conto del titolare** e in base alle normali attribuzioni loro proprie ai sensi della L.R. 44/2003, all'adozione dei provvedimenti di applicazione del D.Lgs. n. 196/2003 nell'ambito delle strutture dirette, con particolare riguardo alla nomina dei responsabili dei trattamenti e alla vigilanza sul rispetto della normativa.

| |
|------------------------------|
| Ruolo dei Direttori generali |
|------------------------------|

Sono inoltre, essi stessi, responsabili del trattamento dei dati personali dei dipendenti regionali assegnati alla loro Direzione generale, nonché dei trattamenti di loro diretta competenza.

I Direttori generali dispongono controlli periodici, anche a campione, e pongono in essere ogni altra azione ritenuta necessaria a verificare il rispetto della normativa. Inoltre, sulla base delle relazioni annuali dei singoli responsabili, predispongono e trasmettono annualmente (entro il 31 gennaio) una relazione di sintesi sullo stato di applicazione della normativa nelle rispettive Direzioni all'Ufficio Privacy Regionale .

L'Ufficio Privacy Regionale, sulla base delle relazioni ricevute da ciascun Direttore generale, a cui, peraltro, fornisce supporto e consulenza, predispone e trasmette alla Giunta Regionale la relazione di sintesi, sullo stato di applicazione della normativa in tutta l'amministrazione regionale, entro il 31 marzo di ogni anno.

4.2.2. RESPONSABILE

I Direttori generali nominano i Responsabili con proprio decreto

I responsabili dei trattamenti di dati personali sono **nominati** dal Titolare (Regione Toscana/Giunta regionale) **per il tramite dei Direttori generali**, che vi provvedono con proprio decreto, indicando analiticamente le funzioni ad essi assegnate (vedi successivo punto 4.2.2.1.).

I dirigenti regionali sono nominati Responsabili del trattamento dei dati personali

I responsabili dei trattamenti di dati personali devono essere individuati, salvo particolari eccezioni, nei dirigenti responsabili delle strutture presso le quali si svolgono i trattamenti, al fine di mantenere coerenza con le responsabilità derivanti dalla L.R. 44/2003 e, dove possibile, con la responsabilità del procedimento amministrativo.

La nomina deve comunque essere fatta esplicitamente.

In caso di mancata designazione dei responsabili dei trattamenti di dati personali, tale responsabilità ricade sui Direttori generali, per i trattamenti di rispettiva competenza.

Per ciascun trattamento deve essere preferibilmente nominato un unico Responsabile interno all'Amministrazione, in modo da evitare una eccessiva frammentazione di responsabilità.

Al fine di semplificare le procedure organizzative, Responsabile del trattamento dei dati personali connesso alla gestione dei sistemi su cui risiedono gli archivi dei diversi trattamenti di dati personali, per funzioni di assistenza tecnica e sistemistica, è designato il dirigente responsabile del competente Settore informatico.

L'elenco completo ed aggiornato dei Responsabili del trattamento all'interno dell'amministrazione regionale è tenuto a cura dell'Ufficio Privacy Regionale, attraverso la procedura informatizzata Trattamento Dati Personali (nel

seguito procedura TDP), nella quale deve essere segnalata, da parte delle strutture competenti ogni modifica di responsabilità in ambito regionale.

La funzione di Responsabile non può essere delegata in nessun caso.

I responsabili possono essere sia interni che esterni all'amministrazione regionale, in relazione alle materie oggetto del trattamento.

Nei casi in cui l'amministrazione regionale si avvalga della collaborazione di soggetti esterni (attraverso contratti, convenzioni, appalti, consulenze, etc.) per l'affidamento di un determinato servizio che comporti come prestazione principale o accessoria un trattamento di dati, il dirigente regionale Responsabile del trattamento provvede a designare e nominare uno o più responsabili esterni per le fasi affidate all'esterno, specificando di effettuare tale nomina **per conto del titolare**.

| |
|--|
| Affidamento all'esterno di trattamenti e nomina dei soggetti esterni a Responsabili per le fasi di loro competenza |
|--|

Tale nomina deve essere inserita nei relativi contratti di affidamento dei servizi, con un'apposita clausola contenente le indicazioni in dettaglio sulle modalità di gestione del trattamento e le misure di sicurezza da adottare.

In tal modo i soggetti esterni si assumono l'onere di operare conformemente alle regole previste dal D.Lgs. 196/2003 e alle disposizioni impartite dalla Regione Toscana in materia di protezione dei dati.

Ciò non toglie la possibilità della nomina del Responsabile esterno da parte del Direttore generale, specie per i casi di maggior rilevanza.

Al fine di garantire omogeneità di comportamento, le strutture regionali che stipulano contratti o convenzioni con strutture e/o soggetti esterni che trattano i dati del titolare Regione Toscana – Giunta Regionale, hanno l'obbligo di raccordarsi con l'Ufficio Privacy Regionale, per concordare il testo dell'atto di nomina del Responsabile esterno, qualora non fosse sufficiente servirsi della modulistica di cui in allegato alla presente Direttiva e consultabile anche nel Sito Intranet regionale dedicato all'area tematica "Privacy".

4.2.2.1. FUNZIONI DEI RESPONSABILI DEI TRATTAMENTI DEI DATI.

I Responsabili devono provvedere al trattamento dei dati personali nel rispetto delle vigenti norme e delle ulteriori disposizioni impartite dal titolare.

Pertanto, per qualsiasi trattamento, il relativo responsabile deve verificare:

- che il trattamento sia connesso con **l'esercizio delle funzioni istituzionali** e che le stesse finalità non siano perseguibili attraverso il trattamento di dati anonimi (principio di **pertinenza** e **principio di necessità**);
- che le modalità del trattamento garantiscano il diritto alla riservatezza dei terzi (principio di **non eccedenza**);
- che il trattamento ed in particolare le modalità adottate **non siano difformi dalle norme di legge e di regolamento**;
- che vengano adottate le **misure di sicurezza**.

| |
|--|
| Principio di necessità, di pertinenza e di non eccedenza |
|--|

Ogni Responsabile del trattamento di dati personali deve verificare periodicamente la sussistenza di tali requisiti con riferimento alle diverse fasi del trattamento, rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

Nel caso in cui l'interessato fornisca spontaneamente dati in eccedenza rispetto a quelli strettamente indispensabili per lo svolgimento delle attività di competenza regionale, tali dati eccedenti possono essere:

- rinviati al mittente,
- distrutti,
- conservati senza utilizzarli,

sulla base della valutazione discrezionale del responsabile del trattamento.

Fra i requisiti suddetti, infatti, assumono particolare rilevanza quelli della **pertinenza** e della **non eccedenza delle informazioni** rispetto alle finalità per le quali i dati personali sono raccolti o trattati.

Ad esempio, il trattamento di alcune informazioni può essere necessario per la fase istruttoria del procedimento

amministrativo, ma può risultare non motivata la loro conoscenza da parte di soggetti diversi da quelli preposti allo svolgimento di compiti specifici. Tale verifica deve comportare, se necessario, la revisione delle modalità organizzative degli uffici e l'adozione di idonee misure di sicurezza.

In particolare i responsabili devono:

- 1) effettuare il censimento dei trattamenti presenti nella propria struttura;
- 2) verificare che i trattamenti in corso o da intraprendere presso la struttura siano rispondenti a quanto disposto dal Codice; ove difforme dalla norma, il trattamento deve essere adeguato o cessare;
- 3) individuare formalmente, secondo quanto specificato al punto 4.2.3., gli incaricati del trattamento dei dati, fornendo loro per iscritto istruzioni circa le modalità del trattamento nel rispetto della legge e di quanto stabilito dal titolare,
- 4) vigilare sulla corretta osservanza delle istruzioni impartite,
- 5) adottare le misure per assicurare la qualità dei dati, le modalità di raccolta e conservazione dei dati, secondo quanto disposto dall'art. 11 della legge e al successivo punto 5 della presente Direttiva,
- 6) adottare misure di sicurezza idonee ad evitare rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, secondo quanto indicato al successivo punto 9 della presente Direttiva,
- 7) rispettare le misure di sicurezza per le banche dati informatizzate contenenti dati personali, di cui al punto 9 della presente Direttiva
- 8) informare per iscritto o oralmente l'interessato o la persona, diversa dall'interessato, presso la quale sono raccolti i dati personali - anche attraverso formule prestampate nel relativo bando pubblicato sul BURT o sulle schede che devono essere compilate dagli interessati - degli elementi previsti dall'art. 13 del D.Lgs. 196/2003 (vedi il successivo punto 7.2. e allegato n. 3).

| |
|--|
| Compiti del Responsabile del trattamento dei dati personali |
|--|

- 9) organizzare la propria struttura per garantire l'esercizio dei diritti dell'interessato, allo scopo di fornire all'interessato, su richiesta, le informazioni previste dall'art. 7 del D.Lgs. 196/2003 nei tempi previsti dalla legge.
- 10) verificare, con riferimento al trattamento di dati sensibili (art. 20) e di dati giudiziari (art. 21), se il trattamento stesso è autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite. Qualora il Responsabile del trattamento accerti in sede di verifica che - pur essendo le rilevanti finalità di interesse pubblico specificate dal D.Lgs.196/2003 o da altra espressa disposizione di legge, manchi un'espressa disposizione di legge che specifichi anche i tipi di dati e le operazioni eseguibili - deve provvedere a:
 - a) identificare i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite;
 - b) comunicare tali informazioni all'Ufficio Privacy Regionale, ai fini degli adempimenti di cui agli artt. 20 – 21 del D.Lgs. 196/2003.Nel caso il Responsabile accerti, in sede di verifica, che le finalità del trattamento non sono previste tra quelle specificate dal D.Lgs. 196/2003 né da espressa disposizione di legge, deve tempestivamente darne comunicazione all'Ufficio Privacy Regionale, che richiederà al Garante il riconoscimento del rilevante interesse pubblico delle attività in oggetto.
- 11) comunicare tempestivamente all'Ufficio Privacy Regionale l'intenzione di avviare nuovi trattamenti non compresi nell'elenco regionale dei trattamenti di dati personali, nonché l'eventuale cessazione di trattamenti in atto, ai fini dell'istruttoria per l'eventuale notificazione al Garante,
- 12) aggiornare l'elenco regionale dei trattamenti,
- 13) trasmettere annualmente al Direttore generale una relazione sull'attività svolta.

4.2.3. INCARICATI

I dirigenti responsabili di trattamento nominano i loro collaboratori incaricati con ordine di servizio.

Nei casi in cui il trattamento dei dati è effettuato, per alcune fasi, da strutture organizzative regionali diverse da quella che fa capo al Responsabile, l'individuazione degli incaricati avviene con disposizione del Responsabile del trattamento dei dati, d'intesa con il dirigente della struttura coinvolta. Quest'ultimo può indicare a tale fine propri collaboratori o se stesso.

Per quanto riguarda i sistemi su cui risiedono gli archivi dei diversi trattamenti di dati personali, il dirigente responsabile del Settore informatico competente provvede, con proprio ordine di servizio, a nominare incaricati i dipendenti assegnati alla sua struttura che accedono ai suddetti sistemi per funzioni di assistenza tecnica e sistemistica.

Nell'impartire le istruzioni, il Responsabile deve prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati, nel rispetto del principio di necessità introdotto dal Codice.

L'atto con cui il responsabile del trattamento individua gli incaricati non va considerato come mero adempimento cui assolvere una tantum, bensì comporta l'impegno del dirigente ad un aggiornamento delle disposizioni, coerente con i mutamenti organizzativi e di assegnazione degli incarichi al personale.

La conoscenza dei dati personali da parte di chi sia stato nominato incaricato non è considerata comunicazione.

| |
|-------------------------------|
| Incaricati del trattamento |
|-------------------------------|

5. DISPOSIZIONI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

Archivio regionale dei trattamenti

5.1. ELENCO REGIONALE DEI TRATTAMENTI DI DATI PERSONALI.

I trattamenti di dati personali effettuati in ambito regionale sono elencati in un apposito Archivio, organizzato con riferimento alle Direzioni generali.

Tale Archivio contiene, per ciascun trattamento: l'indicazione del/dei Responsabile/i, le finalità e modalità del trattamento, la eventuale normativa di riferimento, la natura dei dati trattati (comuni o sensibili), il luogo in cui sono custoditi, le categorie di interessati cui i dati si riferiscono, l'ambito di comunicazione o diffusione dei dati, le misure di sicurezza adottate, l'elenco nominativo degli incaricati individuati per ciascun trattamento, l'indicazione della banca dati cui il trattamento si riferisce, nonché le altre informazioni utili per l'istruttoria ai fini dell'eventuale notificazione /comunicazione al Garante.

L'Archivio regionale dei trattamenti è gestito, nell'ambito del Sistema Informativo in materia di protezione dei dati personali, dalla procedura informatizzata TDP, che consente ai responsabili di trattamento di:

Funzioni dell'Archivio regionale dei trattamenti

- inserire le proposte di modifica dell'archivio (segnalazione di nuovi trattamenti, variazioni rispetto ai trattamenti già presenti in archivio),
- effettuare la segnalazione degli incaricati e dei rispettivi profili, che verrà utilizzata per la creazione dell'Archivio dei profili e per la implementazione del sistema di autorizzazione degli accessi, nonché per la programmazione degli interventi formativi.

I dipendenti non censiti dalla procedura TDP non possono accedere ad alcun archivio di dati personali.

- fornire informazioni sugli strumenti elettronici utilizzati, sui rischi cui è sottoposto il trattamento e le misure in essere e da adottare (allo scopo di inquadrare il trattamento in un profilo di rischio).

È funzione dell'Ufficio Privacy Regionale validare di volta in volta il contenuto dell'Archivio.

Validazione del contenuto dell'Archivio

Per finalità di trasparenza, l'elenco dei trattamenti, con gli elementi descrittivi più significativi relativi a ciascun trattamento, sarà consultabile da parte di tutti gli interessati sul Sito web regionale.

5.2. IL TRATTAMENTO DEI DATI PERSONALI

Secondo quanto disposto dal Codice i dati personali devono essere:

Requisiti di liceità

- trattati in modo lecito e secondo correttezza,
- raccolti e registrati per scopi determinati, espliciti e legittimi ed in funzione dello svolgimento di compiti istituzionali, nei limiti stabiliti dalle leggi e dai regolamenti,
- necessari,
- esatti e, se necessario, aggiornati,
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti,
- 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.

Tali requisiti valgono anche per le copie di scarto dei documenti che sono equiparate ai documenti stessi.

Come trattare le copie di scarto

Ai fini della sicurezza dei dati personali, qualunque prodotto dell'elaborazione di dati personali, ancorché non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, elaborazioni temporanee, etc.), va trattato con le stesse cautele riservate alla versione definitiva.

Pertanto tali materiali, quando non più utili, devono essere sistematicamente distrutti e la loro distruzione deve avvenire in modo controllato e con modalità tale da assicurare il non riutilizzo dei dati.

A tale scopo il Settore competente fornisce alle Direzioni generali lo strumento (macchina distruggi-documenti), per eliminare le copie di scarto, in modo tale da garantire che le

informazioni contenute non siano tecnicamente ricostruibili in alcun modo e non siano accessibili ad altri soggetti non autorizzati al trattamento.

Attualmente la distruzione dei documenti non più validi, segue le regole imposte dalla Legge archivistica del 1963 e dal Codice unico dei beni culturali del 2004 sulle copie di scarto.

Una particolare attenzione deve essere posta nella progettazione e realizzazione dei Sistemi Informativi, i quali, nel rispetto del principio di necessità (art. 3 del Codice), devono essere configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali e identificativi. È necessario infatti evitare il trattamento dei dati personali e dei dati identificativi quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o modalità di identificazione dell'interessato solo in caso di necessità.

Per quanto riguarda le modalità di comunicazione e di trattamento dei dati nell'ambito del Sistema informativo sanitario, l'utilizzo da parte della Regione di dati anagrafici che identificano direttamente l'interessato (nome, cognome, codice fiscale, codice sanitario) è legittimo per le finalità amministrative di competenza regionale, (quali, ad es., la gestione della mobilità sanitaria e relative compensazioni interaziendali e interregionali, l'aggiornamento dell'anagrafe dei cittadini aventi diritto all'assistenza sanitaria, e tutti i trattamenti già previsti dal Regolamento 2006/18/R), mentre risulta non strettamente indispensabile, e quindi viola il principio di necessità di cui all'art.3 del D.Lgs. 196/2003 (Codice Privacy), quando il trattamento di dati è effettuato per le finalità di programmazione, controllo e valutazione dell'assistenza sanitaria.

Per il perseguimento di tali finalità (anche per quanto riguarda la ricostruzione dei percorsi assistenziali, il confronto degli esiti di salute, la valutazione della appropriatezza, dell'efficacia e dell'efficienza dell'assistenza erogata), il collegamento delle informazioni relative ad uno stesso soggetto, presenti nelle diverse basi dati del sistema informativo, può essere effettuato sulla base di un codice univoco (cioè lo stesso per tutte le prestazioni relative ad uno stesso soggetto), tale da non consentire di identificare

direttamente il soggetto (Decreto del Presidente della Giunta Regionale 16 maggio 2006, n. 18/R).

Deve essere comunque possibile la identificazione dei soggetti, con modalità che saranno definite con successivo atto della Giunta regionale, per specifiche esigenze di controllo e verifiche, nelle quali occorre disporre di dati personali relativi ad assistiti identificati.

A questo proposito, la struttura regionale competente nell'ambito del processo trasversale strategico Sistemi Informativi è incaricata di implementare la procedura di attribuzione del codice univoco e di provvedere, esclusivamente nei richiamati casi di necessità espressamente definiti, alla identificazione degli interessati.

I dati provenienti dalle aziende sanitarie sono privati degli elementi identificativi diretti subito dopo la loro acquisizione da parte della Regione, che effettua quindi il trattamento dei dati sulla base del codice univoco.

5.3. COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI COMUNI

Per quanto concerne le operazioni relative alla comunicazione e diffusione il legislatore ha prefigurato una specifica disciplina (art. 19 D.Lgs. 196/2003), differenziata a seconda del soggetto destinatario. Infatti:

- a) la comunicazione **a soggetti privati** o a enti pubblici economici e la diffusione dei dati personali trattati dalla Regione sono ammesse solo se previste da norme di legge o regolamento;
- b) la comunicazione **a soggetti pubblici**, esclusi gli enti pubblici economici, dei dati personali trattati dalla Regione è ammessa:
 - quando è prevista da norme di legge o di regolamento
 - quando, pur mancando una espressa previsione normativa, risulta comunque necessaria per lo svolgimento delle funzioni istituzionali del soggetto richiedente. In tal caso l'amministrazione regionale deve darne comunicazione preventiva al Garante, tramite l'Ufficio Privacy Regionale. Trascorsi 45 giorni, i dati possono essere comunicati al richiedente, salvo

| |
|---|
| Distinzione tra comunicazione dei dati personali a soggetti pubblici e comunicazione a privati o diffusione |
|---|

diversa determinazione del Garante, che peraltro può intervenire anche successivamente.

È fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati.

Non si considera comunicazione lo scambio di dati tra strutture interne all'amministrazione regionale o tra quest'ultime e soggetti esterni individuati come responsabili del trattamento nell'ambito di attività svolte per conto dell'amministrazione sulla base di affidamento di incarico, convenzioni, etc.. In tal caso anche i soggetti esterni che collaborano con la Regione vengono considerati "articolarioni" della stessa.

Esiste un **generale divieto di diffusione dei dati relativi allo stato di salute.**

5.4. DIFFUSIONE DI DATI PERSONALI COMUNI TRAMITE PUBBLICAZIONE SUL B.U.R.T.

Pubblicazione sul BURT

La pubblicazione sul B.U.R.T. di provvedimenti amministrativi contenenti dati personali comuni concretizza un'ipotesi di diffusione degli stessi sia a soggetti pubblici che privati.

Tale pubblicazione è in linea con quanto disposto dell'art.19 del D.Lgs. 196/2003, essendo espressamente prevista dalla legge regionale.

Nell'applicare le disposizioni che stabiliscono le forme e le modalità di pubblicazione sul Bollettino Ufficiale, quali:

- L.R. 20 gennaio 1995 n.9 "Disposizioni in materia di procedimento amministrativo e di accesso agli atti";
- L.R. 15 marzo 1996 n.18 "Ordinamento del Bollettino Ufficiale della Regione Toscana e norme per la pubblicazione degli atti";
- "Direttiva in ordine alla pubblicità degli atti amministrativi regionali e alla loro pubblicazione sul B.U.R.T.", approvata con deliberazione GR n. 262/98,

la struttura redigente deve comunque effettuare una verifica sulla pertinenza e sulla non eccedenza dei dati personali da inserire nell'atto, anche quando di tale atto è prevista la pubblicazione integrale.

L'estensore deve aver cura di inserire i dati personali non strettamente pertinenti al provvedimento, ma necessari per adempimenti successivi (quali, ad es., codice fiscale, coordinate bancarie, conto corrente postale del beneficiario e simili), in un documento allegato (che non viene pubblicato), oppure predisporre, ai fini della pubblicazione dell'atto, un testo nel quale tali dati siano omessi.

Ciò consente di evitare la diffusione di dati personali non necessari alla finalità di trasparenza dell'azione amministrativa sottesa alla pubblicazione.

Le suddette disposizioni non si applicano:

- agli atti regionali che contengono dati personali sensibili, giudiziari ed altri dati particolari (cfr. punto 2.1. e successivi punti 5.6.4. e 5.7.1.)

- agli atti regionali che contengono dati o informazioni che - pur costituendo dato comune ai sensi del Codice - sono compresi nelle fattispecie indicate dall'art.44 LR 9/95 e non possono quindi essere divulgati per motivi di tutela della riservatezza dei terzi.

Tali atti sono esclusi da pubblicità, come specificato al punto 4. della Direttiva n.262/98. In questa ipotesi la struttura redigente dispone la pubblicazione per estremi.

| |
|---|
| Tipologia degli atti e modalità per la loro pubblicazione: pubblicazione per estremi |
|---|

5.5. TRATTAMENTO DI DATI PERSONALI SENSIBILI E GIUDIZIARI.

Il trattamento dei dati sensibili e giudiziari da parte della pubblica amministrazione è soggetto ad una disciplina speciale, individuata, in particolare, dagli articoli 20, 21 e 22 del Codice in materia di protezione dei dati personali.

Inoltre, a tutela della sicurezza dei dati sensibili, sono imposte misure particolarmente rigide, sia per quanto riguarda i presupposti di legittimazione al trattamento e alla comunicazione e diffusione, sia con riferimento alle misure

tecniche, organizzative e logistiche da adottare per il loro trattamento e per la loro conservazione.

5.6. TRATTAMENTO DEI DATI PERSONALI SENSIBILI

Principi applicabili ai trattamenti di dati sensibili (artt. 20, 21, 22)

Il trattamento dei “**dati sensibili**” da parte delle strutture regionali, compresa la loro comunicazione, è consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Nei casi in cui le rilevanti finalità di interesse pubblico non sono individuate da espressa disposizione di legge, occorre fare riferimento al Codice, che individua alcune rilevanti finalità di interesse pubblico per il cui perseguimento è consentito il trattamento di dati sensibili nell’ambito delle relative attività pubbliche (rapporto di lavoro, concessioni, autorizzazioni, agevolazioni, finanziamenti ed altri benefici economici, attività sanzionatoria e di tutela amministrativa e giudiziaria, tutela della salute, tossicodipendenze, ecc.).

Al di fuori delle ipotesi sopraindicate, è possibile richiedere al Garante, nelle more della specificazione legislativa, l’individuazione di eventuali ulteriori attività, tra quelle demandate alla Regione Toscana, che perseguono rilevanti finalità di interesse pubblico, al fine della conseguente autorizzazione al trattamento dei dati sensibili, ai sensi del comma 2 dell’art. 26 del D.Lgs. 196/2003.

Il Garante con il provvedimento con il quale individua le predette attività, ma anche sulla scorta di eventuali verifiche successive, può prescrivere “*misure ed accorgimenti a garanzia dell’interessato che il titolare del trattamento è tenuto ad osservare*”.

5.6.1. ADEGUAMENTO DELL’ORDINAMENTO REGIONALE.

Identificazione dei tipi di dati e operazioni eseguibili

Per i casi in cui, a norma del precedente punto 5.6. risultavano specificate le finalità di rilevante interesse pubblico, ma non i tipi di dati e le operazioni eseguibili, l’amministrazione regionale ha provveduto a identificare e rendere pubblici con atto di natura regolamentare (**Regolamento approvato con DECRETO DEL**

PRESIDENTE DELLA GIUNTA REGIONALE 16 maggio 2006, n. 18/R), adottato in conformità al parere espresso dal Garante su schema tipo, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi.

L'identificazione dei dati e delle operazioni, per l'aggiornamento di tale regolamento, deve essere effettuata dai responsabili dei trattamenti, che ne danno comunicazione all'Ufficio Privacy Regionale, attraverso l'aggiornamento della procedura TDP, per la predisposizione degli atti necessari.

5.6.2. ESCLUSIONE DEL CONSENSO.

Il trattamento da parte della Regione avviene senza il consenso dell'interessato (ad eccezione di quanto indicato al punto successivo) sia per i trattamenti di dati personali sensibili previsti da espressa disposizione di legge, sia per i trattamenti non previsti da espressa disposizione di legge, ma autorizzati sulla base delle disposizioni del Testo Unico relative alle finalità di interesse pubblico da questo individuate.

Esclusione del
consenso

5.6.3. DATI IDONEI A RIVELARE LO STATO DI SALUTE

All'interno della categoria dei dati sensibili, la legge dedica alcune particolari disposizioni al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, che, per la loro particolare delicatezza, sono oggetto di una speciale protezione.

Dati idonei a
rivelare lo
stato di salute

Il trattamento di queste informazioni, infatti, è vietato a livello internazionale e comunitario, ad eccezione di alcuni casi in cui è permesso per perseguire importanti finalità e con specifiche ed elevate garanzie.

Il trattamento dei dati relativi allo stato di salute per finalità amministrative correlate a quelle di prevenzione, diagnosi e cura (art. 85 del D.Lgs. 196/2003) e per le altre finalità di cui all'art. 86, individuate come finalità di rilevante interesse pubblico, avviene senza il consenso dell'interessato, come indicato al precedente punto 5.6.2.

Invece, ai sensi dell'art. 76 comma 1 del Testo Unico, la Regione (come pure gli altri organismi sanitari pubblici), **quando agisce nella qualità di organismo sanitario** (es:

strutture regionali del Sistema Trapianti e TrASFusionale), può trattare i dati idonei a rivelare lo stato di salute **anche in assenza di disposizioni di legge** nelle due fattispecie seguenti:

- a) per il perseguimento di finalità di **tutela dell'incolumità fisica e della salute dell'interessato**, con il consenso dello stesso;
- b) per il perseguimento di finalità di tutela dell'incolumità fisica e della **salute di un terzo o della collettività**, senza il consenso dell'interessato.

In questo caso il trattamento può avvenire previa autorizzazione del Garante. Tale autorizzazione è stata rilasciata dal Garante in via generale e recentemente rinnovata (Autorizzazione n. 2/2005) a valere fino al 30 giugno 2007, salvo ulteriore rinnovo.

| |
|--|
| Trattamento dei dati idonei a rivelare lo stato di salute finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico |
|--|

Il trattamento dei dati idonei a rivelare lo stato di salute finalizzato a **scopi di ricerca scientifica in campo medico, biomedico o epidemiologico** è effettuato di norma con il consenso dell'interessato; il consenso dell'interessato non è necessario quando:

- la ricerca è prevista da un'espressa previsione di legge;
- la ricerca rientra nel programma di ricerca biomedica o sanitaria di cui all'art.12/bis del D.Lgs.502/92 e successive modificazioni (art. 110 del D.Lgs. 196/2003) e per la quale sono trascorsi 45 giorni dalla comunicazione al Garante;
- non è possibile informare gli interessati, ma il progetto di ricerca ha ottenuto il parere favorevole del Comitato etico regionale, ed è autorizzato dal Garante, anche con autorizzazione generale ai sensi dell'art. 40 del Codice.

5.6.3.1. CIFRATURA O SEPARAZIONE DEGLI ALTRI DATI PERSONALI DELL'INTERESSATO

Secondo quanto previsto dal Codice privacy (artt. 22 e 34) i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da ogni altro dato

personale trattato per finalità che non richiedano il loro utilizzo.

I dati sensibili o concernenti provvedimenti giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale, indipendentemente dalle modalità di trattamento, devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi che, considerato il numero e la natura dei dati trattati, permettono di identificare gli interessati solo in caso di necessità.

| |
|--|
| Cifratura e modalità di conservazione per i dati sullo stato di salute |
|--|

L'adozione di tecniche di **separazione dei dati sensibili e giudiziari dai dati identificativi** investe aspetti progettuali del database e quindi risulta preferibile laddove si stia creando un nuovo trattamento dati con relativo database oppure quando i costi in termini di risorse umane ed economiche per l'adozione di tale tecnica siano accettabili. Nel caso di questa tipologia di dati resta comunque necessario mantenere la privacy dei dati, quando questi, eventualmente correlati fra loro, vengono trasferiti fra il sistema centrale ed il client sul quale l'incaricato opera.

I dati personali sensibili o concernenti provvedimenti giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato.

Le operazioni di raffronto fra dati sensibili e/o dati concernenti provvedimenti giudiziari possono essere effettuate solo con l'indicazione scritta dei motivi. Se tali operazioni sono effettuate utilizzando banche dati di diversi titolari, sono ammesse solo se previste da espressa disposizione di legge. (art. 22, comma 10 e 11 del D.Lgs.196/03).

Diffusione dati
sensibili sul BURT

5.6.4. DIFFUSIONE DEI DATI PERSONALI SENSIBILI TRAMITE PUBBLICAZIONE SUL B.U.R.T.

La diffusione dei dati personali sensibili è ammessa solo se prevista da espressa e specifica disposizione di legge (art.22, comma 11, D.Lgs.196/03).

Pertanto, in mancanza di una simile previsione normativa, non è consentita la diffusione tramite pubblicazione sul BURT degli atti amministrativi che contengono dati sensibili; tali atti sono qualificati riservati e pubblicati solo per estremi.

Divieto di diffusione
di dati idonei a
rivelare lo stato di
salute

La diffusione dei dati idonei a rivelare lo stato di salute è vietata; gli atti amministrativi regionali che contengono tali dati devono pertanto essere pubblicati per estremi, (art. 26 comma 5, D.Lgs. 196/2003).

5.7. TRATTAMENTO DEI DATI PERSONALI GIUDIZIARI

Si tratta dei dati idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti (art. 3, comma 1, lettere da a) ad o) e da r) ad u) del DPR 14 novembre 2002 n. 313), oppure la qualità di imputato o di indagato (artt. 60 e 61 del Codice di procedura penale).

Tali dati riguardano:

Dati giudiziari e
loro trattamento

- a) i provvedimenti giudiziari penali di condanna definitivi, anche pronunciati da autorità giudiziarie straniere se riconosciuti ai sensi degli articoli 730 e seguenti del codice di procedura penale, salvo quelli concernenti contravvenzioni per le quali la legge ammette la definizione in via amministrativa, o l'oblazione limitatamente alle ipotesi di cui all'articolo 162 del codice penale, sempre che per quelli esclusi non sia stata concessa la sospensione condizionale della pena;
- b) i provvedimenti giudiziari definitivi concernenti le pene, compresa la sospensione condizionale e la non menzione, le misure di sicurezza personali e patrimoniali, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la

dichiarazione di abitudine, di professionalità nel reato, di tendenza a delinquere;

- c) i provvedimenti giudiziari concernenti le pene accessorie;
- d) i provvedimenti giudiziari concernenti le misure alternative alla detenzione;
- e) i provvedimenti giudiziari concernenti la liberazione condizionale;
- f) i provvedimenti giudiziari definitivi che hanno prosciolti l'imputato o dichiarato non luogo a procedere per difetto di imputabilità, o disposto una misura di sicurezza;
- g) i provvedimenti giudiziari definitivi di condanna alle sanzioni sostitutive e i provvedimenti di conversione di cui all'articolo 66, terzo comma, e all'articolo 108, terzo comma, della legge 24 novembre 1981, n. 689;
- h) i provvedimenti giudiziari del pubblico ministero previsti dagli articoli 656, comma 5, 657 e 663 del codice di procedura penale;
- i) i provvedimenti giudiziari di conversione delle pene pecuniarie;
- l) i provvedimenti giudiziari definitivi concernenti le misure di prevenzione della sorveglianza speciale semplice o con divieto o obbligo di soggiorno;
- m) i provvedimenti giudiziari concernenti la riabilitazione;
- n) i provvedimenti giudiziari di riabilitazione, di cui all'articolo 15 della legge 3 agosto 1988, n. 327;
- o) i provvedimenti giudiziari di riabilitazione speciale relativi ai minori, di cui all'articolo 24 della legge 27 maggio 1935, n. 835;
- r) i provvedimenti giudiziari relativi all'espulsione a titolo di sanzione sostitutiva o alternativa alla detenzione, ai sensi dell'articolo 16 del decreto legislativo 25 luglio 1998, n. 286, come sostituito dall'art. 15 della legge 30 luglio 2002, n. 189;

- s) i provvedimenti amministrativi di espulsione e i provvedimenti giudiziari che decidono il ricorso avverso i primi, ai sensi dell'articolo 13 del decreto legislativo 25 luglio 1998, n. 286, come modificato dall'art. 12 della legge 30 luglio 2002, n. 189;
- t) i provvedimenti di correzione, a norma di legge, dei provvedimenti già iscritti;
- u) qualsiasi altro provvedimento che concerne a norma di legge i provvedimenti già iscritti, come individuato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Ministro della giustizia.

Il trattamento dei dati giudiziari - compresa la loro comunicazione - è ammesso soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichi le rilevanti finalità di interesse pubblico del trattamento stesso, i tipi di dati trattati e le precise operazioni autorizzate.

In relazione alle rilevanti finalità di interesse pubblico individuate dal D.Lgs. 196/2003, i soggetti pubblici devono identificare e rendere pubblici, con le stesse modalità già riportate al precedente punto 5.6.1., anche i tipi di dati e di operazioni oggetto del trattamento concernenti dati giudiziari (artt. 21 e 22, D. Lgs.196/2003).

La diffusione dei dati giudiziari, così come quella dei dati sensibili, è ammessa solo se prevista da espressa disposizione di legge.

5.7.1. DIFFUSIONE DEI DATI GIUDIZIARI TRAMITE PUBBLICAZIONE SUL B.U.R.T.

| |
|---|
| Diffusione dei dati giudiziari tramite BURT |
|---|

Per la diffusione dei dati giudiziari tramite B.U.R.T. valgono le stesse indicazioni fornite per i dati personali sensibili al precedente punto 5.6.4..

5.8. TRATTAMENTI DI DATI PERSONALI PER SCOPI STORICI STATISTICI, E DI RICERCA SCIENTIFICA

Sono di rilevante interesse pubblico le finalità riguardanti i trattamenti di dati personali per scopi storici o effettuati nell'ambito del Sistema statistico nazionale (Sistan) o per scopi scientifici (art. 97, D.Lgs. 196/2003).

Con riferimento ai criteri generali per il trattamento dei dati personali l'art. 99 del D.Lgs. 196/03 precisa che il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati e può essere effettuato anche oltre il periodo necessario a questi ultimi scopi. Questa possibilità deve essere espressamente indicata nell'informativa fornita all'interessato al momento della raccolta dei dati.

Trattamenti per scopi storici, di ricerca scientifica o di statistica

Anche in caso di cessazione del trattamento originario, i dati in oggetto possono essere conservati o ceduti ad altro titolare per scopi storici, di ricerca scientifica e di statistica, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'art. 12 del D.Lgs. 196/03.

5.8.1. TRATTAMENTO DI DATI PERSONALI PER SCOPI STORICI

È considerato un trattamento di "rilevante interesse pubblico" quello effettuato da soggetti pubblici per scopi storici, concernente "finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato".

Trattamento di dati personali per scopi storici

I dati personali raccolti per scopi storici non possono essere usati per adottare provvedimenti contro l'interessato, né per fini diversi da quelli storici. I dati contenuti in documenti storici possono essere utilizzati solo a fini storici e diffusi quando si riferiscono a circostanze o a fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

La consultazione dei documenti conservati negli Archivi è soggetta alle disposizioni di cui al decreto legislativo 29 ottobre 1999, n. 490. In base a questa norma esistono limiti alla consultabilità dei documenti riservati.

Sono quindi esclusi dalla consultazione per 50 anni, in relazione alla data del documento, i documenti "relativi alla politica estera o interna dello Stato" e per 70 anni, quelli "relativi a situazioni puramente private di persone". Un limite di 70 anni alla consultabilità esiste anche per "i documenti dei processi penali", in relazione alla data della conclusione del procedimento.

Trattamento di dati raccolti per scopi statistici e di ricerca

5.8.2. TRATTAMENTO DI DATI RACCOLTI PER SCOPI STATISTICI E DI RICERCA SCIENTIFICA

Gli scopi statistici e di ricerca scientifica devono essere chiaramente determinati e resi noti all'interessato, nei modi di cui all'art.13 del D.Lgs. 196/2003 (vedi successivo punto 7.2. della presente Direttiva).

I dati personali trattati per scopi statistici e di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura.

I dati personali trattati per scopi statistici sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

I dati identificativi, qualora possano essere conservati, sono abbinabili ad altri dati, sempre che l'abbinamento sia temporaneo ed essenziale per i propri trattamenti statistici

Le disposizioni relative al segreto statistico e alla riservatezza dei dati personali non si applicano ai dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Codici di deontologia

5.8.2.1. CODICI DI DEONTOLOGIA E DI BUONA CONDOTTA

In attuazione della normativa sono stati approvati dal Garante:

- Provvedimento 31 luglio 2002 n. 13 "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale"
- Provvedimento 16 giugno 2004 n. 2 "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici"

Tali codici hanno lo scopo di assicurare l'equilibrio tra il diritto alla privacy e le necessità della ricerca scientifica e le ragioni che ne sono alla base: il principio della libertà della ricerca, costituzionalmente garantito, e le esigenze del relativo sviluppo per migliorare le condizioni della società.

Inoltre, i codici completano il quadro delle regole del D.Lgs. 196/03 secondo un ragionevole principio di parsimonia, in base al quale devono essere utilizzati i dati anonimi quando siano sufficienti per gli scopi di una ricerca.

Nei due Codici deontologici sono individuati fra l'altro:

- i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal decreto legislativo 322/89 (vedi successivo punto 5.8.2.2.), siano svolti per idonei ed effettivi scopi statistici e di ricerca scientifica;
- le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire al personale incaricato;
- le misure di sicurezza da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'art.33 del D.Lgs. 196/03.

I responsabili del trattamento dei dati personali dovranno rispettare le disposizioni contenute in tali codici e impartire specifiche istruzioni al riguardo al personale incaricato del trattamento.

5.8.2.2. TRATTAMENTO DI DATI PERSONALI PER FINI STATISTICI NELL'AMBITO DEL PROGRAMMA STATISTICO REGIONALE E NAZIONALE.

I soggetti che fanno parte del Sistema Statistico Nazionale (SISTAN) possono raccogliere ed ulteriormente trattare i dati personali necessari per perseguire gli scopi statistici previsti

| |
|--|
| Trattamento di dati personali per fini statistici nell'ambito del Programma Statistico Nazionale |
|--|

dal decreto legislativo 322/89, dalla legge o dalla normativa comunitaria, qualora il trattamento di dati anonimi non permetta di raggiungere i medesimi scopi.

Per la Regione Toscana la fattispecie di cui sopra si concretizza nei trattamenti effettuati per fini statistici dal Settore Sistema Statistico Regionale, nonché dalle altre strutture regionali limitatamente alle attività previste dal Programma Statistico Nazionale.

I dati personali raccolti per uno specifico scopo statistico (così come quelli raccolti per altri scopi) possono essere trattati dai soggetti sopra indicati per altri scopi statistici di interesse pubblico, se ciò è previsto dal D.Lgs.322/89, dalla legge, dalla normativa comunitaria o da un regolamento. Gli ulteriori scopi statistici devono essere chiaramente determinati e di limitata durata.

5.8.2.3. TRATTAMENTO DI DATI PERSONALI PER FINI STATISTICI E DI RICERCA

Trattamento di dati personali per fini statistici e di ricerca

L'attività statistica e di ricerca al di fuori del SISTAN è disciplinata, oltre che dal D.Lgs. 196/2003, dal citato "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici".

Tale Codice si applica a un'università o altro ente di ricerca o società scientifica, o singolo ricercatore che operi in un'università o ente di ricerca o socio di una società scientifica.

Per quanto riguarda l'ambito regionale il Codice deontologico si applica agli enti regionali di ricerca. Inoltre la Regione Toscana svolge attività di ricerca applicata (vedi scheda 31 del Regolamento dati sensibili e giudiziari, approvato con Decreto del Presidente della Giunta Regionale 16 maggio 2006, n. 18/R)

Il codice deontologico non si applica ai trattamenti per scopi statistici e scientifici connessi con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari.

5.8.2.4. RICERCA SCIENTIFICA IN AMBITO SANITARIO

Con riferimento alla ricerca scientifica in ambito sanitario, in aggiunta alle regole generali sulla ricerca, il quadro normativo si completa con disposizioni aggiuntive.

Ricerca scientifica
in ambito
sanitario

Infatti, per il trattamento di dati idonei a rivelare lo stato di salute per scopi di ricerca scientifica in campo medico, biomedico ed epidemiologico il Codice privacy ha introdotto due norme che affrontano il tema del consenso e quello dell'esercizio dei diritti dell'interessato.

Per il suddetto trattamento il consenso dell'interessato non è richiesto se la ricerca è prevista dalla legge.

Parimenti il consenso non è necessario se la ricerca rientra nel programma di ricerca sanitaria finalizzata (art. 12bis del D.Lgs. 502/1992), ne viene data comunicazione al Garante (cfr. punto 5.6.3.) e, se trascorsi i 45 giorni previsti, si viene ad attuare l'istituto del silenzio-assenso (art. 39 del Codice).

Infine il consenso non è necessario nei casi in cui non sia possibile informare gli interessati, per ragioni particolari, ed il programma abbia ricevuto parere favorevole dal comitato etico competente e sia autorizzato dal Garante.

6. RAPPORTI CON L'AUTORITÀ GARANTE

Ogni rapporto formale o adempimento di legge nei confronti e verso l'Autorità Garante per gli aspetti tecnico-operativi connessi all'attuazione della normativa in ambito regionale, richieste di chiarimenti, richieste di pareri formali, richieste di autorizzazione, comunicazioni, notificazioni, etc., compete al Titolare, il quale vi provvede avvalendosi dell'Ufficio Privacy Regionale, che opera a supporto delle Direzioni generali, allo scopo di evitare frammentazioni.

Rapporti con
l'Autorità Garante

7. ADEMPIMENTI

7.1. NOTIFICAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI.

Notificazione al
Garante

Mentre secondo la L. 675/96 la notificazione era sempre obbligatoria salvo eccezioni, secondo il nuovo Codice (art. 37) il titolare deve notificare al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

- a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazioni di malattie mentali, infettive e diffuse, siero-positività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti.
- e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al

corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

L'attività istruttoria ai fini della notificazione è svolta dall'Ufficio Privacy Regionale, anche con la collaborazione dei Referenti del "Sistema privacy" presso le Direzioni Generali, sulla base delle informazioni fornite dai Responsabili di trattamento tramite la procedura TDP.

7.2. INFORMATIVA AGLI INTERESSATI

Ogni struttura dell'amministrazione regionale assolve agli obblighi di informativa nei confronti dell'interessato ogniqualvolta provvede alla raccolta dei dati personali, informando l'interessato, ai sensi dell'art. 13 del Codice, circa:

Informativa agli
interessati

- le finalità e le modalità del trattamento cui sono destinati i dati richiesti;
- la natura obbligatoria o facoltativa del conferimento di dati richiesti e le conseguenze di un eventuale rifiuto;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'art. 7 del codice;
- la denominazione e la sede del titolare (Regione Toscana – Giunta Regionale) e, se designato, del responsabile, dandone indicazione non nominativa, ma facendo riferimento al responsabile della struttura regionale preposta al trattamento.

L'informativa deve essere preferibilmente resa per iscritto.

In alcuni casi le informative possono essere date con cartelli affissi nei locali in cui gli interessati si recano per conferire i dati (receptions delle sedi regionali, segreterie) o possono essere informative per gli accessi alle pagine Web della Regione Toscana.

Nelle strutture dove sono in funzione degli strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti,

Videosorveglianza

dei visitatori e del patrimonio, deve essere affissa apposita informativa che informi il pubblico della presenza degli impianti e delle finalità perseguite attraverso la videosorveglianza. I pannelli devono essere affissi in prossimità degli ingressi alle strutture ed essere visibili da chi vi accede. E' inoltre necessario rispettare i seguenti principi:

- a) una limitazione delle modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell'immagine), avendo attenzione alla individuazione del livello di dettaglio della ripresa dei tratti somatici delle persone in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;
- b) individuazione dei soggetti legittimati ad accedere alle registrazioni;
- c) indicazione del soggetto e della struttura cui l'interessato può rivolgersi e dei diritti che può esercitare.

Informativa nel caso di dati non raccolti presso l'interessato

Se i dati personali non sono raccolti presso l'interessato, l'informativa è data al medesimo all'atto della registrazione dei dati o non oltre la prima comunicazione ad altri soggetti, se prevista (art. 13, comma 4 del Codice), eccetto nei seguenti casi:

Casi di esonero dal dare l'informativa per i dati non raccolti presso l'interessato

1. quando sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
2. quando sono trattati per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati solo per tale finalità e per il periodo necessario al loro perseguimento;
3. quando l'informativa comporta un impiego di mezzi che il Garante ha dichiarato sproporzionato rispetto al diritto tutelato.

Le sanzioni irrogate dal Garante alla Regione Toscana per omessa o inadeguata informativa all'interessato, graveranno sulla struttura inadempiente responsabile della violazione accertata.

Con riferimento ai trattamenti di competenza della Regione Toscana, si possono prendere in considerazione, per esempio, le seguenti categorie di soggetti "interessati":

- Dipendenti o altri soggetti nell'ambito di un rapporto di lavoro subordinato (amministratori e organi istituzionali di enti controllati, incarichi libero professionali, collaborazioni coordinate e continuative, stages, tirocini, borse di studio, lavoro interinale, volontari per attività di protezione civile, giovani in servizio volontario civile per servizio civile, ecc.):
l'informativa deve essere effettuata al momento dell'instaurazione del rapporto di lavoro (*salvo fornire una tantum l'informativa a tutti i dipendenti in servizio*);
- Fornitori di beni, appaltatori di lavori pubblici e di servizi, consulenti, liberi professionisti (contratti, convenzioni, gare di appalto, incarichi professionali):
l'informativa può essere inserita nel bando di gara o nello schema di contratto/convenzione;
- Soggetti iscritti in albi o elenchi regionali:
l'informativa viene data all'atto dell'iscrizione o dell'aggiornamento degli albi o elenchi,
- Visitatori:
l'informativa consiste in una nota di carattere generale (contenente le finalità e le modalità del trattamento, nonché l'indicazione del Responsabile) esposta presso le sedi regionali aperte al pubblico dove si effettua il ritiro di un documento di identità e la registrazione dei relativi dati.
- Cittadini, persone giuridiche, enti o associazioni destinatari di provvedimenti regionali (ad es. procedimenti relativi alla concessione di contributi, finanziamenti, o altre agevolazioni, rilascio di autorizzazioni o concessioni, ecc...):
l'informativa sul trattamento dei dati che sono acquisiti dalla Regione con riferimento allo specifico procedimento può essere inserita nel relativo bando pubblicato sul BURT, oppure nei modelli da compilare a cura degli interessati.
- Cittadini per quanto riguarda il trattamento dei dati per funzioni istituzionali, non legate a bandi (Servizio sanitario

regionale; Tributi; Rilevazioni statistiche e ricerca; Contenzioso e cause; Studenti):

l'informativa può essere fornita agli interessati con lettera formale o inserita nei modelli da compilare a cura degli interessati o nei questionari di rilevazione o con altre appropriate misure di informazione al pubblico.

Le informative che l'amministrazione regionale è tenuta a predisporre ai sensi del Codice, vengono definite di concerto tra Ufficio Privacy Regionale e Responsabili del trattamento e devono essere redatte sulla base dello schema-tipo allegato alla presente Direttiva (Allegato n. 3) e consultabile nel Sito Intranet regionale dedicato all'area tematica "Privacy".

7.3. DIRITTI DELL'INTERESSATO

I diritti
dell'interessato

Gli uffici e gli Enti regionali devono garantire all'interessato l'esercizio dei diritti di cui all'art. 7 del Codice e precisamente:

1. 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. di ottenere l'indicazione dell'origine dei dati, della logica applicata al trattamento effettuato con mezzi elettronici, degli estremi identificativi del titolare, dei responsabili, dei soggetti o delle categorie di soggetti ai quali i dati possono essere comunicati o che possono venire a conoscenza in qualità di responsabili o incaricati;

3. di ottenere l'aggiornamento, la rettifica o l'integrazione dei dati, 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;

4. di ottenere l'attestazione che le operazioni di cui al precedente n. 3 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 manifesta impossibile o richieda un impiego

di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

5. di opporsi, in tutto o parzialmente, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

7.3.1. ESERCIZIO DEI DIRITTI DELL'INTERESSATO

L'interessato può esercitare i diritti di cui all'articolo 8 del Codice con una richiesta scritta – raccomandata, fax o posta elettronica - al titolare o al responsabile del trattamento.

| |
|--|
| Esercizio dei diritti dell'interessato |
|--|

La richiesta può essere formulata anche oralmente nel caso di esercizio dei diritti di cui all'art. 7 commi 1 e 2 e può essere rinnovata con intervallo non minore di novanta giorni.

Il modulo da utilizzare per l'esercizio dei diritti è il fac-simile di modulo predisposto dall'Autorità Garante (allegato 3 e)), scaricabile dal sito web della Regione Toscana e reperibile presso L'Ufficio Relazioni con il Pubblico, presso l'Ufficio Privacy Regionale o direttamente presso il responsabile del trattamento.

Ai fini dell'esercizio dei diritti l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

I diritti riferiti a dati personali di persone decedute possono essere esercitati da chi ha un interesse proprio ad agire o agisce a tutela della persona deceduta o per ragioni familiari meritevoli di protezione.

L'identificazione dell'interessato è verificata sulla base di idonei elementi. La persona che agisce per conto dell'interessato esibisce o allega copia della procura o della delega sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento proprio e dell'interessato.

I dati sono estratti a cura dell'incaricato e, ove sia possibile, la richiesta presentata dall'interessato viene soddisfatta in via informale e immediata, con comunicazione anche orale ovvero offerta in visione mediante strumenti elettronici. In caso di richiesta, si provvede alla trasposizione dei dati su

supporto cartaceo o informatico ovvero alla trasmissione per via telematica.

Qualora non sia possibile l'accoglimento immediato dell'istanza, il responsabile deve provvedere nel minor tempo possibile, dandone comunicazione scritta all'interessato, e comunque non oltre 30 giorni dalla data di ricevimento della richiesta.

Quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro può avvenire mediante esibizione o consegna in copia di atti e documenti contenenti i dati personali richiesti.

La comunicazione è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di codici o sigle sono forniti elementi per la comprensione del significato.

L'accesso ai dati personali è gratuito. Qualora a seguito della richiesta di cui all'articolo 7, commi 1 e 2, non risulti confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. RAPPORTI TRA LA NORMATIVA SULLA PRIVACY E IL DIRITTO DI ACCESSO.

8.1. ACCESSO AGLI ATTI AMMINISTRATIVI

Rapporto fra privacy e diritto di accesso

Secondo quanto disposto dall'art. 59 del D.Lgs. 196/03, la normativa sul trattamento dei dati personali fa esplicitamente salve le vigenti norme in materia di accesso ai documenti amministrativi.

Sia la giurisprudenza che il Garante per la protezione dei dati personali hanno anzi più volte affermato che la legge di tutela della privacy non può essere presa a pretesto per negare l'accesso agli atti amministrativi.

Per la Regione Toscana, oltre alla L. 241/90, deve farsi riferimento ai seguenti atti legislativi e di indirizzo:

- L.R. 9/1995 “Disposizioni in materia di procedimento amministrativo e di accesso agli atti”;
- Deliberazione G.R. n. 612 del 2.6.1997 “L.R. 9/1995. Disposizioni in materia di procedimento amministrativo e di accesso agli atti - Art. 51 Limitazione al diritto di accesso”;
- Deliberazione G.R. n. 1307 del 2.11.1998 “Direttiva in ordine all’accesso e alla conoscenza dei documenti amministrativi della Regione Toscana” (pubblicata sul supplemento straordinario al BURT n.49/98).

In caso di provvedimenti che contengono dati sensibili, si raccomanda di valutare con attenzione la legittimazione del richiedente. In questo caso, infatti, il soggetto richiedente è legittimato all’accesso – peraltro limitato alla sola visione - solo qualora la conoscenza dell’atto gli sia strettamente necessaria per difendere in giudizio i propri diritti e interessi.

Resta fermo il principio per cui i conflitti tra diritto di accesso e riservatezza dei terzi devono essere risolti nel senso che l’accesso, finalizzato per la cura o la difesa di propri interessi legittimi, prevale rispetto all’esigenza di riservatezza, nei limiti però in cui esso è necessario alla difesa di un interesse giuridicamente rilevante.

Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango pari ai diritti dell’interessato, ovvero è relativa a un diritto della personalità o altro diritto o libertà, fondamentali ed inviolabili.

8.1.1. DIRITTO DI ACCESSO DEI CONSIGLIERI REGIONALI

I consiglieri regionali hanno diritto di ottenere tutte le notizie e le informazioni in possesso degli uffici che siano utili all’espletamento del proprio mandato.

La concreta individuazione da parte degli uffici delle notizie e delle informazioni che possono essere comunicate deve quindi tenere conto di tutto ciò che può essere funzionale allo svolgimento del mandato stesso, e quindi consentire ai consiglieri di valutare con piena cognizione di causa l’operato

| |
|--|
| Diritto di accesso dei consiglieri regionali |
|--|

dell'Amministrazione, di esprimere un voto consapevole sulle questioni sottoposte all'organo consiliare e di promuovere le iniziative di competenza.

In ogni caso, i dati acquisiti dai consiglieri devono essere utilizzati per le sole finalità realmente pertinenti il mandato.

9. MISURE DI SICUREZZA

Tutti i dipendenti, e in particolare gli incaricati del trattamento, devono garantire la sicurezza delle informazioni, attraverso la salvaguardia della loro a) riservatezza, b) integrità e c) disponibilità, e devono attenersi alle "Linee guida" di cui all'allegato 2.

In particolare devono:

- a) assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati ad avervi accesso;
- b) salvaguardare l'accuratezza e completezza delle informazioni e del loro trattamento;
- c) assicurare che gli utenti autorizzati abbiano accesso alle informazioni e ai beni ad esse associati nel momento in cui lo richiedono.

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, ledendo il rapporto di fiducia che deve necessariamente intercorrere tra l'amministrazione regionale e la società civile.

Misure di sicurezza
informatica

Le misure di sicurezza informatica devono tener conto della natura dei dati, delle specifiche caratteristiche del trattamento e delle conoscenze acquisite in base al progresso tecnico. Ai trattamenti devono essere applicate le misure minime di sicurezza, indicate dagli artt. 33-35 del Codice e dettagliate nel Disciplinare tecnico, la loro omissione è punita penalmente, in quanto vi si applica la forma della responsabilità per l'esercizio di attività pericolose.

In sintesi, le misure minime che garantiscono i principi della sicurezza informatica sono:

- utilizzo di un Sistema di autenticazione informatica (User-ID e password) e un sistema di autorizzazione (profili "utente" con potere di accesso);
- adozione di procedure per la custodia di copie di back-up;
- installazione e aggiornamento di software (firewall) per prevenire vulnerabilità rispetto ad attacchi esterni;
- installazione di software antivirus e loro aggiornamento, almeno ogni tre mesi, per il trattamento di dati sensibili, e ogni sei mesi per gli altri dati;
- redazione del documento programmatico per la sicurezza;
- adozione di tecniche di cifratura o codici identificativi per dati sensibili, trattati con strumenti elettronici.

| |
|----------------------------|
| Misure minime di sicurezza |
|----------------------------|

Anche per i trattamenti effettuati senza l'ausilio di mezzi elettronici sono richieste misure minime di sicurezza:

- l'aggiornamento periodico dell'individuazione degli incaricati.
- la previsione di procedure per un'adeguata custodia di atti e di documenti durante tutto il ciclo delle operazioni di trattamento dei dati personali;

Secondo quanto indicato nell'allegato 2, gli incaricati, cui i dati sono affidati per lo svolgimento delle loro mansioni, provvedono a controllare e custodire gli atti cartacei oggetto di trattamento e a restituirli al termine delle operazioni loro affidate.

Durante il trattamento, gli atti e i documenti non dovranno essere lasciati incustoditi; è pertanto opportuno che gli incaricati siano dotati di cassetti o armadi con serratura ove riporre gli stessi in caso di loro assenza temporanea o al termine della giornata, qualora il trattamento non fosse terminato.

A tal fine il responsabile di trattamento segnala l'esigenza alla struttura competente; il settore competente provvede a soddisfare la richiesta.

Finito il trattamento, i documenti dovranno essere restituiti ovvero ricollocati nel posto in cui sono stati prelevati (art. 35 lettera b - allegato B punto 28)

- la previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato;

Per atti e documenti contenenti dati sensibili e giudiziari è invece implicitamente prescritta la conservazione in locali specifici a ciò destinati, che consentano il controllo dell'accesso mediante uno dei seguenti accorgimenti: (a) strumenti elettronici; (b) incaricando alcune persone della vigilanza degli archivi; (c) autorizzando preventivamente chi accede agli archivi (art. 35 lettera c - allegato B punto 29)

- la formazione obbligatoria degli incaricati.

Tale formazione deve essere programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansione.

9.1. SICUREZZA DEGLI ARCHIVI CARTACEI

Archivi cartacei

Anche per i dati personali trattati manualmente devono essere adottate adeguate misure di sicurezza.

Gli archivi cartacei si distinguono in:

- archivi di lavoro: mantenuti a cura dei singoli incaricati negli uffici e nelle aree operative;
- archivio dei fascicoli del personale: archivio ufficiale mantenuto a cura di un Incaricato in locale riservato;
- archivio generale di deposito: archivio mantenuto per motivi storici o per esigenze di legge, mantenuto a cura di uno o più Incaricati in locali di sicurezza.

9.1.1. ARCHIVI DI LAVORO

Archivi di lavoro

Il personale incaricato del trattamento dei dati opera rispettando le istruzioni ricevute per iscritto nell'ordine di servizio di nomina. In particolare segue le seguenti procedure:

- gli armadi, o altre strutture di conservazione, devono essere chiusi a chiave;
- nel corso del trattamento, i documenti sono conservati in appositi contenitori di lavoro chiusi, specie durante le pause di lavoro e quando il personale incaricato deve assentarsi dall'ufficio o dal posto di lavoro;
- eventuali fotocopie devono essere autorizzate dal responsabile e custodite con le stesse modalità dei documenti originali. La loro distruzione deve avvenire in modo controllato e con modalità tale da assicurare il non riutilizzo dei dati.

9.1.2. ARCHIVIO DEI FASCICOLI DEL PERSONALE

Nell'accedere ai documenti cartacei, l'incaricato segue le istruzioni contenute nell'ordine di servizio di nomina. In particolare:

| |
|----------------------------------|
| Archivio fascicoli del personale |
|----------------------------------|

- gli armadi, o altre strutture di conservazione, sono tenuti chiusi a chiave;
- i documenti, chiusi in appositi contenitori di lavoro, sono custoditi in un locale apposito; il locale è presidiato dal personale incaricato, che, durante le proprie pause di lavoro o durante l'assenza dall'ufficio, ha l'obbligo di chiuderlo a chiave;
- i documenti sono prelevati dagli archivi per il tempo strettamente necessario allo svolgimento della mansione;
- eventuali fotocopie devono essere autorizzate e custodite con le stesse modalità dei documenti originali.

9.1.3. ARCHIVIO STORICO (OSMANNORO)

L'Archivio generale risiede in un locale apposito, chiuso a chiave. L'accesso a tale archivio segue le norme previste per

| |
|------------------|
| Archivio storico |
|------------------|

le aree di sicurezza ed è consentito esclusivamente agli incaricati specificatamente autorizzati con ordine di servizio.

9.2. ACCESSO AI DATI PARTICOLARI

Per il trattamento di dati sensibili o attinenti ai dati giudiziari, l'accesso ai dati è determinato sulla base di **autorizzazioni assegnate dal Responsabile agli incaricati del trattamento o della manutenzione**, singolarmente o per gruppi di lavoro. Periodicamente, e comunque almeno una volta l'anno, il Responsabile deve verificare la sussistenza delle condizioni per la loro conservazione.

L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.

9.3. ADEMPIMENTI RELATIVI AI FORNITORI CHE POSSONO VENIRE A CONOSCENZA DI DATI PERSONALI

Adempimenti verso i fornitori esterni

Il Titolare Regione Toscana per garantire che il personale di ditte fornitrici, che si trovi ad intervenire presso l'amministrazione regionale, o che operi nell'ambito di forniture che trattino qualsiasi tipologia di dati personali, operi nel rispetto delle vigenti disposizioni in materia di protezione dei dati personali, adotta le seguenti idonee misure:

1. in base a quanto disposto dal D.L. 196/2003 – Allegato B, punto 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." Deve quindi essere fatta esplicita e formale richiesta di redazione di opportuno rapporto di intervento ogni volta che questo sia dovuto, da redigere in modalità conforme alla vigente normativa, che dovrà essere controfirmato da un rappresentante del Settore competente all'atto della consegna;

2. In base a quanto previsto ai punti 1, 2, 3, 4, 6 dell'Allegato B, del D.L. 196/2003 è indispensabile procedere alla nomina di incaricati di tutti quei soggetti che hanno accesso al sistema informativo regionale a fini manutentivi o più in generale per erogare il servizio oggetto di fornitura o che in ogni caso trattino dati personali che ricadono sotto le competenze del Titolare Regione Toscana – Giunta Regionale. A tal fine il fornitore deve essere nominato responsabile esterno e a sua volta deve individuare il personale coinvolto nel trattamento e procedere a formale incarico, con l'individuazione dei compiti specifici che tale personale dovrà svolgere presso le sedi regionali. Qualora i soggetti interessati cessino di svolgere, definitivamente o comunque per un periodo superiore a sei mesi, le funzioni per le quali hanno ricevuto l'incarico, dovrà esserne data tempestiva comunicazione alla struttura regionale interessata, che provvederà a revocare i diritti di accesso ai locali e ai sistemi.

9.4. DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Gli articoli da 33 a 36 del "Codice", nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, prevedono che i titolari del trattamento adottino le misure minime individuate dal "Codice" medesimo, volte ad assicurare un livello minimo di protezione dei dati personali.

Documento
Programmatico
per la sicurezza

Nel caso di trattamenti di dati sensibili o di dati giudiziari effettuato con l'ausilio di strumenti elettronici, nell'ambito delle misure minime di sicurezza da adottare, rientra anche la predisposizione del Documento Programmatico sulla Sicurezza (DPS).

La Giunta Regionale, in attuazione della normativa in materia di privacy, con **Delibera n. 1259 del 27/12/2005** ha approvato il Documento Programmatico per la Sicurezza, che dovrà essere aggiornato entro il 31 marzo di ogni anno.

A tal fine l'Ufficio Privacy Regionale dà comunicazione del suddetto atto di approvazione alla Direzione Generale Bilancio e Finanze, che riferisce nella relazione accompagnatoria del bilancio di esercizio dell'avvenuta redazione o aggiornamento del DPS (art. 34 del Codice e disposizione n. 26 del Disciplinare tecnico o Allegato B).

La nuova disciplina privacy infatti al punto 26 dell'Allegato B) del Codice dispone che *"Il titolare riferisce, nella relazione accompagnatoria del bilancio di esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico"*.

Ciascun responsabile di trattamento è tenuto ad adottare le misure di sicurezza previste nel Documento Programmatico sulla Sicurezza per quanto di propria competenza, sulla base delle responsabilità individuate nel Documento stesso.

ALLEGATI

ALLEGATO 1

“Misure di sicurezza relative al trattamento di dati personali, ruoli e funzioni nella struttura organizzativa del Titolare Giunta Regionale.”

Ufficio Privacy Regionale

Per “Ufficio Privacy Regionale” - (UPR) – si intende l’insieme di funzioni in materia di protezione dei dati personali svolte all’interno di una struttura regionale che è già esistente. L’UPR è titolare del processo trasversale denominato “Sistema Privacy”, pertanto:

- coordina e presidia tutte le funzioni connesse all’attuazione della specifica normativa,
- definisce i parametri di standardizzazione, garantendo continuità e unitarietà di indirizzo,
- risponde alle contingenti necessità operative/funzionali delle singole Direzioni Generali.
- cura i rapporti con l’ufficio dell’Autorità Garante – per gli adempimenti formali e sostanziali previsti dalla normativa, in qualità di referente per l’Amministrazione Regionale.

L’Ufficio Privacy regionale, per adempiere alle proprie funzioni, si avvale delle risorse assegnate e dei Referenti del “Sistema privacy” presso le Direzioni Generali.

Settore Infrastrutture e Tecnologie per lo Sviluppo della Amministrazione Elettronica

Il Settore Infrastrutture e Tecnologie per lo Sviluppo della Amministrazione Elettronica:

- gestisce i servizi Internet;
- gestisce i sistemi centrali;

- emana le direttive per quanto riguarda i prodotti software da installare sulle macchine, in particolare per l'adozione di strumenti antivirus validi ed aggiornati;
- emana le direttive per quanto riguarda i prodotti hardware da installare sulle macchine;
- istruisce adeguatamente i referenti informatici affinché possano svolgere correttamente il loro lavoro;
- garantisce la sicurezza informatica e telematica, onde evitare eventuali usi non corretti degli account;
- gestisce la Certification Authority;
- gestisce la cooperazione applicativa.

Amministratori di sistema e gestori di servizi

Svolgono le seguenti attività:

- aggiornano il Sistema Operativo o il software applicativo per i server;
- aggiornano tempestivamente le macchine con le patches che eliminano bugs noti;
- essere iscritti alle liste che consentono di venire a conoscenza di eventuali bugs che, in assenza di patch possono portare all'interruzione del servizio;
- eseguono backup periodici dei dati;
- eseguono backup dei pacchetti applicativi e del sistema operativo quando vengono fatti aggiornamenti o nuove installazioni;
- adottano particolari misure di sicurezza per i supporti di backup al fine di prevenire eventi di distruzione o di accesso non autorizzato;
- per i sistemi più critici adottano tecnologie che consentono di mantenere in linea una copia sempre aggiornata dei dati (mirroring o RAID);
- prevedono l'accesso ai sistemi tramite identificazione (login) ed autenticazione (password); in particolare il

login deve essere univoco per ogni utente e la password nota solo all'utente stesso; persone che lavorino sugli stessi dati e/o procedure devono avere login e password diverse;

- gestiscono l'accesso ai sistemi con privilegi diversi, in modo che i vari utenti accedano solo alle risorse hardware e software che gli competono;
- svolgono attività di auditing ovvero di monitoraggio, registrazione ed interpretazione degli eventi al fine di individuare anomalie e tentativi di violazione della sicurezza.
- segnalano al responsabile della sicurezza informatica e telematica eventuali situazioni anomale.

Referenti informatici

Ai referenti informatici sono assegnati i seguenti compiti:

- Gestione dei computers della propria Direzione Generale
- Supporto nella risoluzione di eventuali problemi
- Gestione della strumentazione informatica della propria Direzione Generale

Settore Sistemi Informativi e Servizi per lo Sviluppo dell'Amministrazione Elettronica

Il Settore Infrastrutture e Tecnologie per lo Sviluppo della Amministrazione Elettronica:

- progetta, realizza, integra e provvede a mantenere i sistemi informativi di settore;
- progetta e promuove servizi di amministrazione elettronica per favorire l'inclusione delle categorie economiche e delle libere professioni nella società dell'informazione e della comunicazione programmazione, realizzazione e coordinamento di progetti di e-

government riferiti alle categorie economiche e alle libere professioni;

- attiva processi di semplificazione e diffusione delle ICT (Information Communication Tecnology) per accrescere il livello della competitività del sistema regionale.

ALLEGATO 2

“Linee guida per gli utenti in merito alle Misure Minime di Sicurezza”

1. UTILIZZATE LE CHIAVI

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che un armadio chiuso a chiave può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per aprirlo. Quando vi allontanate dal vostro ufficio, chiudete i documenti a chiave nei cassetti e/o negli armadi.

2. CONSERVATE I SUPPORTI ESTRAIBILI (FLOPPY-DISK, CD-ROM, CHIAVI USB, ETC.) IN UN LUOGO SICURO

Per i supporti estraibili si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che non contengano dati personali, riponeteli sotto chiave non appena avete finito di usarli.

3. UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.

- a) La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
- b) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.

- c) La password del salva-schermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di accedere alle risorse del vostro computer.

4. COME DEVE ESSERE SCELTA LA PASSWORD

La parola chiave per l'accesso al sistema deve essere composta da almeno otto caratteri e nel caso il sistema non lo consenta da un numero di caratteri massimo consentito; la parola chiave non deve contenere caratteri riconducibili all'incaricato ed è modificata al primo utilizzo e successivamente ogni sei mesi; per il trattamento dei dati sensibili e giudiziari la parola chiave deve essere modificata ogni tre mesi.

5. NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

6. CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

7. PER EVITARE LA IDENTIFICAZIONE DELLA PASSWORD

- a) NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
- b) NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
- c) Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.

- d) NON scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile “provare” tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- e) NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- f) NON usate il Vostro nome utente. È la password più semplice da indovinare
- g) NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

8. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

9. NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

10. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

11. NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÀ

Personale esterno può avere bisogno di installare un nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

12. NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegati in rete offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la Rete, ed è quindi vietato. Per l'utilizzo di altri apparecchi, consultatevi con il responsabile del trattamento dati del vostro ufficio e con il referente informatico.

13. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il responsabile del trattamento dati e con il referente informatico.

14. PER GARANTIRE IL RIPRISTINO DEI DATI EFFETTUARE DEI BACKUP PERIODICI.

I vostri dati potrebbero essere gestiti da un *file server*, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup, oppure salvati su un supporto removibile (cd-rom, floppy-disk, etc.)

15. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

CHE COS'È UN VIRUS:

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME *NON* SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da dischetti;
3. Quando si scaricano dati o programmi da Internet.

ALCUNI EFFETTI PROVOCATI DA VIRUS:

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inespugnabilmente;

COME PREVENIRE I VIRUS:

1. USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA DISCHETTO

Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

3. PROTEGGETE I VOSTRI DISCHETTI DA SCRITTURA QUANDO POSSIBILE

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

4. ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con il responsabile del trattamento dati e con il referente informatico per maggiori dettagli .

COME EVITARE DI DIFFONDERE I VIRUS:

5. NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA

Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignorateli: le e-mail di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da un vostro parente o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli *hoax* più diffusi).

6. NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

ALLEGATO 3

Modulistica/Fac-Simile

a) **Informativa ex art. 13 D.lgs. 196/2003**

(Da inserire in fondo al modello di raccolta dati)

Gentile Signore/a,

Desideriamo informarLa che il D.lgs. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali") prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.

Ai sensi dell'articolo 13 del D.lgs. n.196/2003, pertanto, Le forniamo le seguenti informazioni:

1. I dati da Lei forniti verranno trattati per le seguenti finalità:

2. Il trattamento sarà effettuato con le seguenti modalità:

.....

(Indicare le modalità del trattamento: manuale / informatizzato / altro.)

3. Il conferimento dei dati è facoltativo/obbligatorio (se obbligatorio, specificare il motivo dell'obbligo) e l'eventuale rifiuto di fornire tali dati non ha alcuna conseguenza / potrebbe comportare la mancata o parziale esecuzione del contratto / la mancata prosecuzione del rapporto.

(Scegliere l'opzione adeguata alla situazione)

4. I dati non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione

o

i dati potranno essere / saranno comunicati a: o diffusi presso:

(Scegliere l'opzione in funzione del trattamento ed indicare, se

presente, l'ambito di comunicazione e/o diffusione).

Se nel trattamento sono coinvolti anche dati sensibili, occorre integrare la dichiarazione:

Il trattamento riguarderà anche dati personali rientranti nel novero dei dati "sensibili", vale a dire dati 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]. I dati sanitari potranno essere trattati da centri medici specializzati nel valutare l'idoneità al lavoro

.....
(scegliere la categoria che interessa).

sarà effettuato con le seguenti modalità:
.....
.

I dati in questione non saranno comunicati ad altri soggetti né saranno oggetto di diffusione

o
i dati potranno essere / saranno comunicati a:o
diffusi presso:

(Scegliere l'opzione a seconda delle caratteristiche del trattamento e indicare, se presente, l'ambito di comunicazione e/o diffusione, gli estremi della legge che ne dà l'autorizzazione, fermo restando il divieto relativo ai dati idonei a rivelare lo stato di salute, di cui all'art.26, comma 5 del D.lgs. 196/2003).

La informiamo che il conferimento di questi dati è facoltativo/obbligatorio *(se obbligatorio, specificare il motivo dell'obbligo)* e l'eventuale rifiuto a fornirli non ha alcuna conseguenza/potrebbe comportare la mancata o parziale esecuzione del contratto/la mancata prosecuzione del rapporto/.

5. Il titolare del trattamento è: Regione Toscana – Giunta Regionale

6. Il responsabile del trattamento è il responsabile del Settore /Area..... Direzione generale _____
(indicare almeno un responsabile, e, se designato ai fini di cui all'art.7 del D.lgs.196/2003, indicare tale responsabile del trattamento; indicare, inoltre, il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili)

7. Gli incaricati del trattamento sono i dipendenti assegnati alla struttura del responsabile;

8. In ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art.7 del D.lgs.196/2003.

Allegato 3

b) Ordine di servizio del/della dirigente responsabile del Settore



REGIONE TOSCANA
Giunta Regionale

Direzione Generale
Via cap..... Firenze
Tel. 055/..... Fax. 055/.....
e-mail

Ordine di servizio del/della dirigente responsabile del Settore

.....
Numero **del**

Oggetto: Nomina degli incaricati dei trattamenti di dati personali di competenza del settore

.....

IL/LA DIRIGENTE

Visto il D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" che ha abrogato la L. 31 dicembre 1996, n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" e successive modifiche e integrazioni;

Visto il decreto del Direttore generale della Direzione generale n. del, con il quale il/la sottoscritto/a ha assunto la responsabilità dei trattamenti di dati personali di competenza del Settore, secondo quanto specificato nel citato decreto;

Vista la delibera della Giunta regionale n. del avente ad oggetto "Direttiva per l'attuazione del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" ed in particolare il punto 4) che prevede che il dirigente nomini con propria disposizione gli incaricati del trattamento dei dati

qualora questi ultimi siano individuati nell'ambito dei collaboratori assegnati alla struttura organizzativa che fa capo al responsabile del trattamento dei dati;

DISPONE

di nominare incaricati dei trattamenti dei dati personali relativi all'attività del Settore in oggetto (per le operazioni che ciascun dipendente svolge per propria competenza), così come risulta dall'elenco trattamenti sottoindicati, fornendo loro le istruzioni allegate al presente ordine di servizio.

Trattamento _____

| Incaricati | Per le operazioni relative a: |
|------------|-------------------------------|
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |
| _____ | _____ |

A) Istruzioni per il trattamento dei dati personali di competenza del Settore da parte degli incaricati dei trattamenti

Il trattamento dei dati da parte dei dipendenti formalmente incaricati dovrà avvenire nel rispetto dei criteri di cui all'art. 11 del D.Lgs. 196/2003 e delle ulteriori disposizioni impartite con Direttiva della Giunta Regionale. L'accesso ai dati è consentito per quanto strettamente necessario per adempiere ai compiti individualmente assegnati, con divieto di qualunque diversa utilizzazione, funzione e divulgazione non espressamente autorizzata dal Responsabile del trattamento.

In particolare, per quanto riguarda le elaborazioni e le altre fasi dei trattamenti effettuate attraverso i personal computer collegati alla rete regionale, ciascun incaricato disporrà di una parola chiave per l'accesso ai dati e un codice identificativo personale.

Gli incaricati avranno cura di :

- non condividere il proprio codice identificativo personale con altri utenti (a meno che non sia espressamente previsto);
- non cedere a terzi la propria parola chiave di autenticazione;
- non accedere a servizi loro non consentiti;
- non caricare ed eseguire software di rete o di comunicazione senza previa verifica dello stesso da parte del proprio Referente Informatico che opera in stretto rapporto con l'Area di Coordinamento Reti di Governance del Sistema Regionale e Ingegneria dei Sistemi Informativi e della Comunicazione;
- non tentare di acquisire privilegi di amministratore di sistema;
- non collegare modem o comunque dispositivi che consentano un accesso non controllato ad apparati della rete privata di Regione Toscana;
- effettuare il *backup* periodico dei propri dati di interesse.

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati devono essere conservati dagli incaricati per la durata del trattamento e successivamente conservati in archivi ad accesso controllato, secondo quanto sarà indicato di volta in volta.

Nel caso di trattamento di dati sensibili o di dati giudiziari, gli atti e i documenti contenenti i dati affidati agli incaricati del trattamento devono essere conservati in contenitori muniti di serratura.

Gli incaricati sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto.

Analogamente, per quanto riguarda i flussi di documenti cartacei all'interno degli uffici regionali, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse).

I/La Dirigente Responsabile

.....

Partecipato a:

.....

Allegato 3

c) Nomina del responsabile esterno

TRATTAMENTO DEI DATI PERSONALI

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali, emanata con il D.Lgs. 30 giugno 2003, n. 196, ed in relazione alle operazioni che vengono eseguite per lo svolgimento delle attività previste dall'incarico indicato in oggetto, la Regione Toscana – Giunta Regionale, in qualità di Titolare, nomina la (Società o Raggruppamento, Università o altro) Responsabile esterno del trattamento, ai sensi dell'art. 29 e secondo quanto previsto dalla Direttiva adottata con Deliberazione della Giunta Regionale n. del

Si precisa che tale nomina avrà validità per il tempo necessario per eseguire le operazioni affidate dal titolare e si considererà revocata a completamento dell'incarico.

Il soggetto (Società o Raggruppamento, Università o altro), in quanto responsabile esterno, è tenuto ad assicurare la riservatezza delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione, impegnandosi a rispettare rigorosamente tutte le norme relative all'applicazione del D.Lgs 196/2003.

In particolare si impegna a:

- utilizzare i dati solo per le finalità connesse allo svolgimento dell'attività oggetto del contratto con divieto di qualsiasi altra diversa utilizzazione;
- nominare per iscritto gli incaricati del trattamento, fornendo loro le necessarie istruzioni;
- adottare idonee e preventive misure di sicurezza atte ad eliminare o, comunque, a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell'articolo 31 del D.Lgs. 196/03;

- adottare tutte le misure di sicurezza, previste dagli articoli 33, 34, 35 e 36 del D.Lgs. 196/03, che configurano il livello minimo di protezione richiesto in relazione ai rischi di cui all'articolo 31, analiticamente specificate nell'allegato B al decreto stesso, denominato "Disciplinare tecnico in materia di misure minime di sicurezza";
- informare gli interessati, al momento della raccolta dei dati, secondo quanto previsto dall'art. 13 del D.Lgs. 196/2003, sulle finalità della rilevazione e relativo titolare e sulla natura facoltativa o obbligatoria del conferimento dei dati;
- predisporre e trasmettere alla Regione Toscana una relazione conclusiva in merito agli adempimenti eseguiti, con cadenza annuale oppure ogni qualvolta ciò appaia necessario;
- trasmettere tempestivamente e, comunque non oltre le 24 ore successive al loro ricevimento, i reclami degli Interessati e le eventuali istanze del Garante.

(Nel caso non sia già stata data l'informativa al soggetto destinatario dell'incarico, inserire la seguente formula direttamente nell'atto di nomina a responsabile esterno)

Informativa art.13 Codice in materia di protezione dei dati personali

In relazione al trattamento dei Suoi dati personali, ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali (D.Lgs n.196/2003), si informa inoltre che i dati da Lei forniti verranno trattati dalla Regione Toscana per le finalità connesse al conferimento dell'incarico e che non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione.

Si ricorda che in ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art.7 del D.lgs.196/2003.

Allegato 3

d) Esercizio dei diritti dell'interessato

Vedi MODELLO GARANTE PER ESERCIZIO DEI DIRITTI

Allegato 3

e) Accesso al registro dei trattamenti tenuto dal Garante per la protezione dei dati personali

Luogo,Data

AL GARANTE DELLA PROTEZIONE DEI DATI PERSONALI

Oggetto: Decreto Legislativo 196/2003 (Codice in materia di trattamento dei dati personali). Esercizio del diritto di accesso ai dati personali ed altri diritti, di cui all'art. 7.

Io sottoscritto, nato a, il, residente in....., rivolgo cortese istanza al fine di conoscere, mediante accesso gratuito al registro di cui all'art. 154, comma 1, lettera L del D. Lgs. 196/2003, l'esistenza di trattamenti di dati che possono riguardarmi.

A tali fini, specifico che

.....
.....
(indicare le peculiarità del proprio lavoro, famiglia, stato civile, attività effettuate, appartenenza a circoli, corrispondenza intrattenuta con aziende, mezzi di trasporto utilizzati, acquisti, etc., dalle quali si possa individuare l'ambito di trattamenti che possono essere rilevanti).

In attesa di cortese riscontro, porgo distinti saluti

Nome, Cognome, Indirizzo, Firma leggibile

NOTE:

1. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse

2. Nell'esercizio dei diritti, l'interessato può dare delega o procura scritta a persone fisiche o associazioni. In tal caso, la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso.