INDICE

3	Introduzione
Parte I^	
4	1. Finalità e principi generali del D.lgs. 196/2003
4	2. Definizioni
	2.1. Dati
	2.2. Operazioni
	2.3. Soggetti
	2.4. Misure di sicurezza
	2.5. Ulteriori definizioni
Parte II^	
7	3. Ambito di applicazione
7	4. Modalità e disposizioni organizzative della Regione Toscana
	4.1. Soggetti che trattano i dati personali
	4.1.1. Titolare
	4.1.2. Responsabile
	4.1.2.1. Funzioni dei responsabili dei trattamenti dei dati
	4.1.3. Incaricati
	4.2. Amministratori di sistema
	4.3. Il Sistema Privacy
	4.3.1. Ufficio Privacy Regionale
	4.3.2. I referenti del Sistema Privacy
11	5. Disposizioni generali per il trattamento dei dati personali
	5.1. Archivio regionale dei trattamenti di dati personali
	5.2. Il trattamento dei dati personali
	5.3. Comunicazione e diffusione dei dati comuni
	5.3.1. Diffusione di dati comuni tramite pubblicazione sul B.U.R.T. e sulla banca dati degli atti
	5.4. Trattamento di dati sensibili e giudiziari
	5.4.1. Trattamento dei dati sensibili
	5.4.1.1. Dati idonei a rivelare lo stato di salute
	5.4.1.2. Comunicazione dei dati idonei a rivelare lo stato di salute alle forze di polizia
	5.4.1.3. Il trattamento dei dati personali nel Sistema informativo sanitario
	5.4.1.4. Funzione di correlazione anagrafica
	5.4.2. Trattamento dei dati giudiziari
	5.4.3. Diffusione dei dati sensibili e giudiziari tramite pubblicazione sul B.U.R.T. e sulla banca dati degli atti
	5.5 Diffusione dei dati personali tramite pubblicazione sulla sezione "Amministrazione trasparente" del sito istituzionale
	5.6. Trattamenti di dati personali per scopi statistici, storici e di ricerca scientifica
	5.6.1. Trattamento di dati personali per scopi storici
	5.6.2. Trattamento di dati raccolti per scopi statistici e di ricerca scientifica
	5.6.2.1. Codici di deontologia e di buona condotta
	5.6.2.2. Trattamento di dati personali per fini statistici nell'ambito del Programma Statistico Regionale e Nazionale

- 5.6.2.3. Trattamento di dati personali per fini statistici e di ricerca
- 5.6.2.4. Ricerca scientifica in ambito sanitario

- 19 6. Rapporti con l’Autorità Garante per la protezione dei dati personali
- 19 7. Adempimenti
 - 7.1. Notificazione al Garante
 - 7.2. Comunicazione al Garante
 - 7.3. Informativa agli interessati
 - 7.4. Diritti dell'interessato
 - 7.4.1. Esercizio dei diritti dell'interessato
- 22 8. Rapporti tra la normativa sulla privacy e il diritto di accesso.
 - 8.1. Accesso agli atti amministrativi
 - 8.1.1. Diritto di accesso dei consiglieri regionali
- 23 9. Misure di Sicurezza
 - 9.1. Sicurezza degli archivi cartacei
 - 9.1.1. Archivi di lavoro
 - 9.1.2. Archivio dei fascicoli del personale
 - 9.1.3. Archivio storico (Osmannoro)
 - 9.2. Accesso ai dati particolari
 - 9.3. Adempimenti relativi ai fornitori che possono venire a conoscenza di dati personali
 - 9.4. Documento annuale per la sicurezza dei dati personali

Parte III^

- 27 ALLEGATI
 - Allegato n.1
“Linee guida per gli utenti in merito alle Misure Minime di Sicurezza”
 - Allegato n.2
“Sistema Privacy” – Procedure organizzative

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

INTRODUZIONE

La Pubblica Amministrazione per lo svolgimento delle proprie attività istituzionali ha necessità di acquisire e trattare dati personali operando con sistemi elettronici e di comunicazione sempre più integrati ed interconnessi. Ciò rende fondamentale lo sviluppo di una cultura della sicurezza delle informazioni e della tutela dei diritti degli interessati.

Il termine "privacy" - comunemente usato per indicare la riservatezza delle informazioni - deve essere interpretato alla luce del concetto di "protezione dati personali", con il quale il legislatore riconosce il diritto a trattare le informazioni personali soltanto nell'ambito di specifiche regole previste dall'ordinamento, contenute nel decreto legislativo n. 196 del 30 giugno 2003, denominato "Codice in materia di protezione dei dati personali", che raccoglie in un quadro sistematico la normativa statale sulla privacy uniformandosi a quella comunitaria.

La presente Direttiva fornisce indirizzi e modalità organizzative per la Regione Toscana e costituisce 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.

La Direttiva rappresenta inoltre uno strumento operativo per i vari soggetti che assumono ruoli di responsabilità nel trattamento dei dati personali. In particolare mira a fornire a dirigenti ed 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.

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

La Direttiva si articola in tre sezioni:

- una Parte I introduttiva, 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 e a promuovere;
- una Parte III costituita dagli allegati.

Per facilitarne la reperibilità, il testo è disponibile nella Intranet nella sezione "privacy", e sul sito web della Regione Toscana all'indirizzo: <http://www.regione.toscana.it/cittadini/diritti-e-cittadinanza/privacy>

PARTE I[^]

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

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, delle libertà fondamentali e 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.

In base all'art. 3 del Codice, che introduce il principio di necessità, si prevede 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.

Questo principio integra e completa quelli di pertinenza e non eccedenza, in base ai quali i dati possono essere trattati soltanto se completi, funzionali e non eccessivi rispetto agli scopi legittimi perseguiti (art.11 Codice privacy).

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 strumenti situati in Italia (anche diversi da quelli elettronici), salvo che si tratti di un "mero transito di dati nell'UE".

Le norme del Codice non si applicano ai trattamenti di dati personali effettuati da persone fisiche per fini esclusivamente personali (a meno che tali dati non siano destinati ad una comunicazione sistematica o alla diffusione), ai dati delle persone giuridiche, enti e associazioni (la tutela dei dati personali riguarda solo le persone fisiche), infine il Codice non trova applicazione qualora il trattamento riguarda "dati aggregati" o "dati anonimi".

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

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.

Il Codice prevede un diverso regime tra soggetti privati e pubblici.

- I soggetti pubblici non devono richiedere il consenso dell'interessato, tranne nel caso in cui il trattamento dei dati sia effettuato da 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; l'eventuale acquisizione del consenso non legittima l'amministrazione a trattare i dati per finalità diverse da quelle istituzionali o a effettuare operazioni non consentite da leggi o regolamenti.
- I soggetti privati e gli enti pubblici economici devono invece richiedere il consenso per trattare i dati degli interessati.

2. DEFINIZIONI

Le definizioni adottate dalla presente direttiva sono quelle previste dall'art. 4 del D.Lgs n. 196/2003.

2.1. Dati

Il "dato personale" è qualunque informazione relativa a persona fisica, identificata o identificabile in modo diretto o indiretto.

All'interno di questa definizione più generale si specificano ulteriori tipologie di dati:

a) i "dati identificativi" sono i dati personali che permettono l'identificazione diretta dell'interessato;
b) 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.

L'elenco dei dati sensibili è chiuso: infatti sono da considerarsi tali solo ed esclusivamente 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.)

c) 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 (vedi anche punto 5.4.2)

d) dati che, per semplicità, si è soliti definire "dati comuni" sono tutti i restanti dati personali, non compresi nelle precedenti categorie b) e c); (es.: dati anagrafici, coordinate bancarie, codice fiscale).

e) i "dati anonimi" sono i dati che, in origine o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

La classificazione di cui sopra 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'interessato derivante da un eventuale illecito trattamento.

2.2. Operazioni

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.

Particolare attenzione il Codice dedica alla comunicazione e alla diffusione, a cui viene attribuito il seguente significato:

- 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.
- 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.

2.3. Soggetti

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

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, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

b) Il "responsabile del trattamento" è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposta 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 è facoltativa.

- c) Gli "incaricati" del trattamento sono i soggetti che effettuano materialmente le operazioni. Possono essere individuati quali incaricati solo le persone fisiche. Sono nominati per iscritto dal titolare, o dal responsabile se nominato, 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 indicato, 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.

- d) L'"interessato" è la persona fisica cui si riferiscono i dati personali.

- e) Il "Garante" è l'autorità di cui all'articolo 153 del Codice, preposta alla protezione dei dati personali.

2.4. Misure di sicurezza

Le misure di sicurezza sono articolate in due gruppi correlati, il primo inserito nel corpo del Codice dagli articoli 31 a 36, che prevede le regole generali; il secondo riportato in allegato nel "Disciplinare tecnico" o "Allegato B", che contiene dettagliate prescrizioni e le procedure da seguire per garantire il rispetto delle norme del Codice.

Le misure di sicurezza si distinguono in:

- "misure minime", ovvero 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;

- "misure idonee", volte a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti in relazione al livello di sviluppo tecnologico raggiunto.

In particolare, ai fini dell'applicazione delle misure minime richieste, si evidenzia la distinzione fra trattamenti effettuati con strumenti elettronici e trattamenti "cartacei".

Ulteriori definizioni nell'ambito delle misure di sicurezza sono:

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

2.5. Ulteriori definizioni

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-Giunta regionale in applicazione dei principi di cui al D.Lgs. 196 del 30 giugno 2003 in materia di protezione dei dati personali, di seguito denominato "Codice".

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

4.1. Soggetti che trattano i dati personali in Regione Toscana

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

4.1.1. Titolare

Con deliberazione della Giunta Regionale n. 208 del 9.3.1998 l'ente "Regione Toscana -Giunta Regionale" è stato individuato 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.

Il Titolare provvede ad assolvere agli obblighi previsti dalla normativa nazionale in materia di protezione 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 Codice
- 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.

I Direttori generali della Giunta regionale provvedono, per conto del titolare e in base alle normali attribuzioni loro proprie ai sensi della L.R. 1/2009, all'adozione dei provvedimenti di applicazione del Codice nell'ambito delle strutture dirette, con particolare riguardo alla nomina dei responsabili dei trattamenti e alla vigilanza sul rispetto della normativa.

Sono inoltre essi stessi responsabili dei trattamenti di dati personali di loro diretta competenza.

Al fine di verificare il rispetto della normativa, i Direttori generali possono disporre controlli periodici, anche a campione, e pongono in essere ogni altra azione ritenuta necessaria.

4.1.2. Responsabile

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

I responsabili interni 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. 1/2009 e, dove possibile, con la responsabilità del procedimento amministrativo.

Sono nominati dal titolare Regione Toscana/Giunta regionale, per il tramite dei Direttori generali, che vi provvedono con decreto contestualmente al conferimento dell'incarico dirigenziale, indicando analiticamente le istruzioni a cui si devono attenere per il trattamento dei dati personali (così come previsto dal comma 5 art. 29 del Codice).

A tal fine, i decreti di conferimento degli incarichi dirigenziali dei direttori generali dovranno prevedere:

- un espresso capoverso relativo all'attribuzione della responsabilità del trattamento dei dati personali, che a titolo esemplificativo può essere il seguente: "di attribuire, per conto del Titolare Regione Toscana - Giunta

Regionale, a..... la responsabilità dei trattamenti dati personali, ai sensi dell'art.29 del D.Lgs 196/2003, relativamente alle attività e funzioni dallo stesso presidiate, stabilendo che adottati, nell'ambito della struttura dirigenziale diretta, le disposizioni e le misure attuative del 'Codice in materia di protezione dei dati personali', secondo le previsioni contenute nella direttiva regionale di cui alla delibera di G.R. n..... e nel rispetto delle istruzioni di cui all'allegato A, parte integrante del presente provvedimento;"

- un apposito allegato, contenente le istruzioni per il responsabile (reperibile nella intranet regionale – sezione privacy – modulistica).

I trattamenti di dati personali afferenti a ciascun responsabile devono essere appositamente censiti nella procedura informatizzata Trattamento Dati Personali (procedura TDP), che integra e completa la nomina del responsabile e che pertanto deve sempre essere aggiornata ed attuale.

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

L'elenco completo ed aggiornato dei Responsabili all'interno della Regione Toscana-Giunta regionale, nonché dei trattamenti attribuiti a ciascuno di essi, è mantenuto a cura della struttura competente in materia di privacy, di seguito denominata Ufficio Privacy Regionale, attraverso la procedura informatizzata Trattamento Dati Personali (procedura TDP), nella quale deve essere tempestivamente registrata da parte dei Settori competenti ogni variazione di competenze e della conseguente responsabilità di trattamento dei dati. La funzione di responsabile non può essere delegata in nessun caso.

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, per le funzioni di assistenza tecnica e sistemistica relative alla gestione degli archivi dei trattamenti dei dati personali, il responsabile è individuato nel dirigente del competente Settore in materia di infrastrutture tecnologiche.

Nei casi in cui la Regione Toscana 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 nominare uno o più responsabili esterni, specificando di effettuare tale nomina per conto del titolare.

I contratti di affidamento dei servizi, con un'apposita clausola, devono contenere tale nomina, le indicazioni in dettaglio sulle modalità di gestione del trattamento. In tal modo i soggetti esterni si assumono l'onere di operare conformemente alle regole previste dal Codice e alle disposizioni impartite dalla Regione Toscana.

Al fine di garantire omogeneità di comportamento, le strutture regionali che stipulano contratti o convenzioni con strutture e/o soggetti esterni, sono tenute a raccordarsi con l'Ufficio Privacy Regionale, per concordare il testo dell'atto di nomina del Responsabile esterno, qualora non fosse sufficiente servirsi della modulistica consultabile nella sezione Intranet regionale dedicata all'area tematica "Privacy".

4.1.2.1. Funzioni dei responsabili dei trattamenti dei dati

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

Pertanto, per qualsiasi trattamento, il 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.

Ogni responsabile deve verificare periodicamente la sussistenza di tali requisiti nelle 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, i dati eccedenti possono essere

distrutti o 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.

I Responsabili devono:

- 1) effettuare il censimento dei trattamenti presenti nella propria struttura;
 - 2) verificare che i trattamenti in corso o da intraprendere siano rispondenti a quanto disposto dal Codice e, ove difforme, adeguare o cessare il trattamento;
 - 3) individuare formalmente, secondo quanto specificato al punto 4.1.3., gli incaricati del trattamento, 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, le modalità di raccolta e conservazione dei dati;
 - 6) adottare le misure di sicurezza per quanto di propria competenza;
 - 7) informare per iscritto o oralmente l'interessato o la persona diversa dall'interessato, presso la quale sono raccolti i dati personali, degli elementi previsti dall'art. 13 del Codice;
 - 8) organizzare la propria struttura per garantire l'esercizio dei diritti dell'interessato (accesso ai propri dati personali, rettifica, aggiornamento, cancellazione, opposizione al trattamento);
 - 9) 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 verifichi che il Codice o la legge individuino espressamente le rilevanti finalità di interesse pubblico ma non 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 Codice.
- Qualora, invece, il Responsabile verifichi che le finalità del trattamento non sono previste tra quelle specificate dal Codice 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;
- 10) comunicare tempestivamente all'Ufficio Privacy Regionale l'intenzione di avviare nuovi trattamenti non compresi nell'elenco regionale dei trattamenti di dati personali, ai fini dell'istruttoria per l'eventuale notificazione al Garante, nonché l'eventuale cessazione di trattamenti in atto;
 - 11) aggiornare l'elenco regionale dei trattamenti (Procedura TDP). L'aggiornamento dell'archivio dei trattamenti e la nomina degli incaricati costituisce adozione delle misure minime di sicurezza la cui mancata adozione comporta le sanzioni previste dagli artt. 162 comma 2 bis (sanzione amministrativa da 10.000 a 120.000 euro) e 169 del Codice (arresto fino a 2 anni).

4.1.3. Incaricati

I dirigenti responsabili di trattamento nominano i loro collaboratori (dipendenti assegnati al settore e soggetti che operano ad altro titolo sotto la sua diretta autorità), incaricati con ordine di servizio.

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.

Il Responsabile è tenuto ad aggiornare la nomina dei propri incaricati contestualmente con i mutamenti organizzativi della propria struttura.

4.2. Amministratori di sistema

Gli Amministratori di sistema (Provvedimenti Garante del 27/11/2008 e del 25/06/2009) sono figure professionali dedicate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad esempio gli amministratori di dominio e di server) per effettuare trattamenti di dati personali e altre figure, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, equiparabili ai primi dal punto di vista dei rischi relativi alla protezione dei dati personali. Non rientrano invece in tale definizione coloro che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software (per es. per scopi di manutenzione a seguito di guasti o malfunzionamenti).

Funzioni tipiche degli amministratori di sistema sono:

- 1 . organizzazione dei flussi di rete
- 2 . manutenzione hardware
- 3 . realizzazione di copie di sicurezza
- 4 . custodia delle credenziali di autenticazione
- 5 . gestione dei sistemi di autenticazione e autorizzazione
- 6 . gestione dei supporti di memorizzazione

Nello svolgimento dei compiti loro assegnati, gli amministratori di sistema devono attenersi alle regole tecniche, previste nel disciplinare tecnico di cui al DD 1252 del 06.04.2011.

L'elenco degli amministratori di sistema con i nominativi e gli ambiti di operatività in funzione dei profili autorizzativi assegnati, deve essere aggiornato annualmente dal dirigente responsabile in materia di infrastrutture tecnologiche, previa valutazione delle caratteristiche di esperienza, capacità ed affidabilità dei soggetti.

Nel caso in cui il servizio di amministratore di sistema di competenza della Giunta Regionale sia esternalizzato, il responsabile esterno deve predisporre un documento con gli estremi identificativi e gli ambiti di operatività delle persone fisiche preposte quali amministratori di sistema. Tale documento deve essere trasmesso al competente settore della Giunta regionale e reso disponibile in caso di accertamento da parte del Garante. La redazione dell'elenco degli amministratori di sistema deve essere espressamente prevista nella clausola contrattuale o nell'atto di designazione del responsabile esterno.

4.3. Il Sistema Privacy in Regione Toscana

Per "Sistema Privacy" si intende il processo organizzativo determinato dall'insieme di modalità, attività e relazioni che attengono al trattamento e alla protezione dei dati personali e che coinvolgono la Regione Toscana, sia nei rapporti interni, sia nei rapporti che intercorrono con il sistema degli enti, delle agenzie, aziende e altri organismi pubblici dipendenti, ai sensi art.50 Statuto.

I soggetti principalmente coinvolti nei processi organizzativi descritte nell'Allegato 2 sono l' Ufficio privacy Regionale ed il Referente del Sistema Privacy presso le direzioni generali.

4.3.1. Ufficio Privacy Regionale

Per "Ufficio Privacy Regionale" (UPR) si intende l'insieme di funzioni in materia di protezione dei dati personali svolte all'interno della competente struttura regionale.

L'UPR è titolare del processo organizzativo "Sistema Privacy", e come tale:

- fornisce indirizzi, linee guida, consulenze e supporto tecnico alle strutture e agli enti regionali,
- cura i rapporti con l'Ufficio del Garante per la protezione dei dati personali,
- cura, per conto del titolare Regione Toscana – Giunta regionale, gli adempimenti previsti dal Codice ed in particolare la comunicazione e la notificazione al Garante e la redazione e l'aggiornamento del regolamento regionale per il trattamento dei dati sensibili e giudiziari;
- cura l'aggiornamento del Documento annuale per la sicurezza dei dati personali
- vigila sull'osservanza della normativa sulla privacy

- coordina e vigila sull'aggiornamento dell'Archivio regionale dei trattamenti dei dati personali (archivio TDP)
- richiama i Responsabili dei trattamenti a verificare la coerenza dei trattamenti censiti nell'archivio TDP.

Nell'esercizio delle competenze di cui ai punti precedenti l'Ufficio Privacy Regionale si avvale della collaborazione dei Referenti del "Sistema Privacy".

4.3.2. Referente del Sistema Privacy

Il Referente del Sistema Privacy, che è nominato presso ciascuna direzione generale con ordine di servizio del direttore, operando in stretto raccordo con l'UPR, svolge le seguenti funzioni:

- assicura l'assistenza interna alla direzione generale, per il corretto adempimento della normativa sulla privacy
- collabora con il responsabile del trattamento per formulare richieste di parere all'UPR
- supporta i responsabili nell'aggiornamento dell'Archivio TDP per i trattamenti di competenza della direzione generale
- verifica che nei decreti del Direttore Generale relativi al conferimento di nuovi incarichi dirigenziali o a riassetto organizzativi che comportano variazioni sulle responsabilità dirigenziali sia prevista anche la nomina degli stessi dirigenti a "responsabili dei trattamenti dati personali" connessi alle funzioni assegnate, come previsto al punto 4.1.2.

Inoltre è tenuto a segnalare all'UPR i casi in cui presso la propria direzione generale occorra:

- aggiornare il regolamento regionale per il trattamento dei dati sensibili e giudiziari con ulteriori trattamenti
- valutare la necessità di procedere alla notificazione di un trattamento al Garante ex art 37 del Codice
- chiedere all'UPR di provvedere alla Comunicazione al Garante ex art. 39 del Codice nel caso in cui vi sia una richiesta di trasmissione di dati comuni da parte di soggetti pubblici non prevista dalla legge.

5. DISPOSIZIONI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

5.1. Archivio regionale dei trattamenti di dati personali

I trattamenti di dati personali effettuati in ambito regionale sono elencati nell'Archivio TDP che contiene, per ciascun trattamento:

- la Direzione Generale competente,
- l'indicazione del Responsabile,
- le finalità e modalità del trattamento,
- la normativa di riferimento,
- la tipologia dei dati trattati,
- 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,
- ogni altra informazione utile per l'istruttoria ai fini dell'eventuale notificazione /comunicazione al Garante.

L'Archivio TDP è gestito, nell'ambito del portale di Accesso Sicuro denominato ARPA, dalla procedura informatizzata TDP, nella quale i responsabili di trattamento devono:

- 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 di accesso;

- 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).

Per finalità di trasparenza, l'elenco dei trattamenti, con gli elementi descrittivi più significativi è consultabile da parte di tutti gli interessati sul sito web istituzionale di Regione Toscana.

5.2. Il trattamento dei dati personali

Regione Toscana tratta i dati personali per lo svolgimento delle funzioni istituzionali e senza il consenso dell'interessato (art. 18 comma 2 del Codice).

Secondo quanto disposto dall'art. 11 del Codice i dati personali devono essere:

- 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,
- esatti e aggiornati,
- pertinenti, completi e non eccedenti rispetto alle finalità per i 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.

Ai fini della sicurezza, 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.

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 con opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

5.3. Comunicazione e diffusione dei dati comuni

Per quanto concerne le operazioni relative alla comunicazione e diffusione il legislatore ha prefigurato una specifica disciplina (art. 19 Codice), 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 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'UPR. Trascorsi 45 giorni, i dati possono essere comunicati al richiedente, salvo diversa determinazione del Garante, che peraltro può intervenire anche successivamente.

È fatta salva la comunicazione 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 (art. 25 Codice).

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 "articolazioni" della stessa.

Esiste un tassativo divieto di diffusione dei dati relativi allo stato di salute (art. 22 comma 8 Codice) e dei dati inerenti la vita sessuale (combinato disposto art. 22 e art. 60 Codice)

5.3.1. Diffusione di dati comuni tramite pubblicazione sul B.U.R.T. e sulla banca dati degli atti

La pubblicazione sul B.U.R.T. e sulla banca dati degli atti di provvedimenti amministrativi contenenti dati comuni costituisce il caso tipico di diffusione degli stessi. Tale pubblicazione è in linea con quanto disposto dall'art.19 del Codice, essendo espressamente prevista dalla legge regionale n. 23 del 23.04.2007; deve inoltre rispettare le prescrizioni contenute nelle "Linee Guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" emanate dall'Autorità Garante Privacy il 2 marzo 2011.

Nell'applicare le disposizioni che stabiliscono le forme e le modalità di pubblicazione la struttura redigente deve sempre 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, e deve aver cura di inserire i dati personali non strettamente pertinenti al provvedimento, ma necessari per adempimenti successivi (quali, ad es., 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 pubblicazione.

5.4. Trattamento di dati sensibili e giudiziari

Per il trattamento dei dati sensibili e giudiziari da parte della pubblica amministrazione 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. Le disposizioni da applicare sono quelle previste agli articoli 20, 21 e 22 del Codice.

Secondo quanto previsto dal Codice (artt. 22, comma 7 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, 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 (art. 22 comma 6).

I dati sensibili e 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 giudiziari possono essere effettuate solo con l'indicazione scritta dei motivi. Quando si utilizzano banche dati di diversi titolari, l'interconnessione o raffronto sono ammessi solo se previsti da espressa disposizione di legge (art. 22, comma 11).

5.4.1 Trattamento dei dati sensibili

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 finalità di rilevante interesse pubblico non sono individuate da espressa disposizione di legge, occorre fare riferimento al Codice, che tipizza alcune finalità di rilevante interesse pubblico per il cui perseguimento è consentito il trattamento di dati sensibili da parte delle pubbliche amministrazioni (accesso – art. 59; registri stato civile, anagrafi, liste elettorali – art. 62; concessioni, autorizzazioni, agevolazioni, finanziamenti ed altri benefici economici, attività sanzionatoria e di tutela amministrativa e giudiziaria – artt.64- 73; tutela della salute, tossicodipendenze, ecc.- artt.85-86; istruzione e formazione – art.92; trattamenti per scopi storici, statistici o scientifici – art. 98; rapporto di lavoro – art.112).

Qualora le finalità di rilevante interesse pubblico non siano espressamente previste da disposizioni di legge, è possibile richiedere al Garante l'individuazione delle ulteriori attività, tra quelle demandate a Regione Toscana, che perseguono finalità di rilevante interesse pubblico, al fine di ottenere l'autorizzazione al trattamento. Il Garante comunica l'autorizzazione entro 45 giorni, decorsi i quali la mancata pronuncia equivale a rigetto.

Per i casi in cui la legge specifica 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 DPGR 12 febbraio 2013, n. 6/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.

5.4.1.1 Dati idonei a rivelare lo stato di salute

All'interno della categoria dei dati sensibili, la legge dedica alcune 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.

Il trattamento dei dati relativi allo stato di salute per finalità amministrative correlate a quelle di prevenzione, diagnosi e cura (art. 85 del Codice) e per le altre finalità di cui all'art. 86, individuate come finalità di rilevante interesse pubblico, avviene senza il consenso dell'interessato.

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, che non è necessario nelle ipotesi contemplate dall'art. 110 del Codice.

5.4.1.2. Comunicazione di dati idonei a rivelare lo stato di salute alle forze di polizia

In applicazione dell'art. 25, comma 2, del Codice Privacy, per le richieste di dati inerenti lo stato di salute degli interessati effettuate da forze di polizia o dall'autorità giudiziaria per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, non trova applicazione l'art. 20 del Codice Privacy, in base al quale tale operazione può aver luogo solo qualora prevista in una norma di legge o di regolamento, che specifichi anche i tipi di dati oggetto di comunicazione.

Il Titolare Regione Toscana-Giunta regionale individua il dirigente responsabile del sistema informativo sanitario quale responsabile della comunicazione ex art.25 comma 2 del D.Lgs 196/2003, sia per i dati anagrafici che per quelli sanitari, conservati in ottemperanza alle disposizioni del Codice Privacy in archivi separati.

Il responsabile del sistema informativo sanitario, a fronte di richieste formali inerenti la comunicazione di dati sanitari – previamente sottoposte alla valutazione del settore competente per gli aspetti giuridici e legali della D.G. Diritti di cittadinanza e coesione sociale-, pervenute da forze di polizia o dall'autorità giudiziaria per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, procede a richiedere al responsabile dell'Anagrafe regionale degli assistibili l'esecuzione della funzione di correlazione anagrafica, a partire dai dati anagrafici oggetto della richiesta e a individuare conseguentemente le prestazioni sanitarie oggetto della richiesta associate al codice identificativo ricevuto, comunicandole infine all'autorità richiedente.

Il processo relativo all'effettuazione della comunicazione è il seguente:

- 1 - il Richiedente (forza di polizia/autorità giudiziaria) chiede alla DG DCCS di conoscere eventi sanitari di una persona, e fornisce il codice fiscale della persona stessa;
- 2 - il Responsabile del sistema informativo sanitario, o un suo incaricato, inoltra la richiesta del codice univoco, correlato ai dati che ha ricevuto, al Responsabile dell'Anagrafe regionale degli assistibili, comunicandogli i seguenti contenuti:
 - codice fiscale del soggetto
 - data inizio e data fine intervallo indagine
 - indirizzo del richiedente
 - tipologia indagine (ospedaliera o ambulatoriale)
 - motivazione dell'indagine
- 3 - il Responsabile dell'Anagrafe regionale degli assistibili, o suo incaricato, genera un progressivo di richiesta (es. n. 1 del 23/6/2013) ed esegue l'estrazione del codice univoco.
- 4 - il Responsabile dell'Anagrafe regionale degli assistibili, o suo incaricato, invia comunicazione al Richiedente contenente il progressivo richiesta
- 5 - il Responsabile dell'Anagrafe regionale degli assistibili, o suo incaricato, invia comunicazione alla DG DCCS con i seguenti contenuti:
 - codice univoco
 - progressivo richiesta
 - data inizio e data fine intervallo indagine
 - indirizzo del richiedente

- tipologia indagine (ospedaliera o ambulatoriale)
- motivazione dell'indagine

6 - il Responsabile del sistema informativo sanitario, o suo incaricato, estrae le informazioni sanitarie della tipologia indicata per il codice univoco comunicato

7 - il Responsabile del sistema informativo sanitario, o suo incaricato, invia comunicazione al Richiedente con progressivo richiesta e dati estratti

8 - il Responsabile del sistema informativo sanitario, o suo incaricato, invia comunicazione al Responsabile dell'Anagrafe regionale degli assistibili, o suo incaricato, per conferma chiusura.

5.4.1.3 Il trattamento dei dati personali nel Sistema Informativo Sanitario

Un caso particolare di trattamento di dati personali e sensibili è costituito dal Sistema Informativo sanitario. In questo ambito, 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 Decreto del Presidente della Giunta Regionale 12 febbraio 2013, n. 6/R "Regolamento di attuazione dell'art. 1, comma 1, della l.r. 3 aprile 2006, n. 13 "Trattamento dei dati sensibili e giudiziari da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo"), mentre risulta non strettamente indispensabile, e quindi viola il principio di necessità, quando il trattamento di dati è effettuato finalità di programmazione, controllo e valutazione dell'assistenza sanitaria.

Per il perseguimento di tali finalità (in particolare per 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 l'interessato.

I dati provenienti dalle aziende sanitarie sono comunicati alla Regione già privati degli elementi identificativi diretti; pertanto Regione, per le finalità sopra evidenziate, effettua il trattamento dei dati anonimizzati mediante l'assegnazione di un codice univoco

5.4.1.4 Funzione di correlazione anagrafica

Nei casi in cui ricorrano specifiche esigenze di controllo e verifiche ai sensi dell'art. 8 octies Dlgs 502/92 e dell'art. 88, comma 2, L.388/2000, è consentita l'associazione fra gli eventi sanitari e i dati anagrafici degli interessati. Tale operazione è possibile grazie alla funzione di correlazione anagrafica, che si realizza mediante una tabella di correlazione anagrafica, che contiene un identificativo associato alla scheda anagrafica e un secondo identificativo, diverso dal primo, associato alle schede che contengono dati sanitari; il secondo identificativo individua sempre la stessa persona nei vari flussi informativi di dati sanitari, ma attraverso di esso non si può risalire all'identità dell'interessato se non tramite il corrispondente identificativo associato alla scheda anagrafica.

La funzione di correlazione anagrafica è reversibile. Infatti, dato un codice univoco è sempre possibile, mediante una opportuna query sulla base dati anagrafica, recuperare il codice fiscale e i dati anagrafici di una persona.

I soggetti autorizzati ad effettuare questa operazione di decodifica sono le persone incaricate del trattamento ai sensi dell'art.30 del Codice privacy dal dirigente responsabile della tenuta dell'Anagrafe sanitaria regionale, previa richiesta formale dei responsabili delle funzioni di controllo e verifica ai sensi dell'art.8 octies del D.lgs.502/1992 e dell'art.88 comma 2 della Legge 388/2000.

5.4.2 Trattamento dei dati 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:

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.

Non sono considerati dati giudiziari i provvedimenti di cui alle lettere p) e q) del predetto art.3 DPR 313/2002 (sentenze dichiarative di fallimento; decreto di chiusura del fallimento; decreto di omologazione del concordato fallimentare e delle sentenze di interdizione, inabilitazione e revoca) in quanto in queste ipotesi prevale l'esigenza di pubblicità rispetto alla tutela della riservatezza.

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 finalità di rilevante interesse pubblico del trattamento stesso, i tipi di dati trattati e le operazioni eseguibili. Analogamente a quanto previsto per il trattamento dei dati sensibili, qualora la legge individui soltanto le finalità di rilevante interesse pubblico, le p.a. devono identificare i tipi di dati e di operazione oggetto del trattamento tramite un atto di natura regolamentare (DPGR 6/R/2013), adottato anche su schema-tipo previo parere di conformità del Garante (art. 21 Codice) .

5.4.3 Diffusione dei dati sensibili e giudiziari tramite pubblicazione sul B.U.R.T. e sulla banca dati degli atti

La diffusione dei dati sensibili e giudiziari è ammessa solo se prevista da espressa e specifica disposizione di legge (art.22, comma 11, Codice).

La diffusione dei dati idonei a rivelare lo stato di salute (art. 22, comma 8, Codice) e dei dati inerenti la vita sessuale (combinato disposto art. 22 e art. 60 Codice) è sempre vietata.

Quando l'atto amministrativo contiene dati sensibili o giudiziari esclusi da pubblicazione ai sensi della normativa sopra citata, la struttura redigente, ove possibile, provvede ad inserire i dati personali sensibili/giudiziari in un documento allegato (che non viene pubblicato), provvedendo alla pubblicazione

dell'atto in banca dati/BURT, oppure, quando tali dati sono indispensabili per la finalità dell'atto, dispone la "pubblicazione per estremi in banca dati" dell'atto stesso (alcune categorie di atti per i quali va esclusa la pubblicazione sono indicate al punto 6.1 dell'allegato alla DGR 148 del 03.03.2014).

5.5 Diffusione dati personali tramite pubblicazione sulla sezione "Amministrazione trasparente" del sito istituzionale.

La disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (D.lgs. 33/2013) dispone che Regione Toscana pubblichi nella home page del sito istituzionale la sezione "Amministrazione trasparente", al cui interno sono contenuti tutti i documenti, le informazioni ed i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, come previsto dal d.lgs. citato, concernenti l'organizzazione e l'attività dell'amministrazione.

Le modalità di pubblicazione individuate agli artt. 6 e 7 del citato decreto, devono essere tali da consentire a chiunque un accesso diretto ed immediato ai dati e ai documenti, di fruirne gratuitamente e di poterli riutilizzare, nel rispetto delle disposizioni e dei limiti del Codice Privacy.

I dati e i documenti in detta sezione sono pubblicati per un periodo di 5 anni (art. 8 d.lgs. 33/2013), con decorrenza dall'anno solare successivo a quello da cui decorre l'obbligo di pubblicazione e comunque sino a quando gli atti producono effetti giuridici, fatto salvo quanto diversamente disposto (es. artt. 14 comma 2 e 15 comma 4 del d.lgs. 33/13).

Oggetto di pubblicazione obbligatoria ai sensi del d.lgs. 33/2013 sono solo i dati comuni. Pertanto la pubblicazione di dati sensibili e giudiziari può aver luogo solo se prevista da una espressa disposizione di legge, come disposto dall'articolo 22, comma 11 del Codice.

Lo stesso D. Lgs. 33/2013 nell'art. 4 fissa i limiti alla trasparenza e, per quanto riguarda in particolare i dati personali, esclude sempre la pubblicazione dei:

- dati idonei a rivelare lo stato di salute e la vita sessuale;
- dati personali dei dipendenti relativi alla natura delle infermità o degli impedimenti personali o familiari che causino l'astensione dal lavoro;
- i dati personali esclusi dall'accesso ex art. 24 comma 1 l. 241/1990;
- i dati personali coperti da segreto statistico ex art. 9 l. 322/1989;

E' inoltre esclusa la pubblicazione (art. 26, comma 4, d.lgs. 33/2013) dei dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione delle sovvenzioni, contributi, sussidi ed ausili finanziari, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati.

In tal caso le strutture sono tenute a provvedere alla pubblicazione dell'elenco dei beneficiari di tali contributi e sovvenzioni sostituendo il dato identificativo o con le iniziali o con un numero progressivo.

A titolo meramente esemplificativo, rientrano in tale casistica gli atti adottati in base alla:

- legge regionale 2.8.2013, n. 45 "Interventi a sostegno finanziario in favore delle famiglie e dei lavoratori in difficoltà, per la coesione e per il contrasto al disagio sociale"
- legge regionale 27.10.2008, n. 57 "Fondo di solidarietà per familiari vittime di incidenti mortali sul luogo di lavoro"
- legge regionale 20.11.2006, n.55 "Interventi a favore delle vittime del terrorismo e della criminalità organizzata".

Ai sensi dell'art.4, co 3, D. Lgs. 33/2013 Regione Toscana può disporre la pubblicazione di ulteriori atti e documenti oltre a quelli già previsti dal decreto medesimo o da altra previsione di legge o di regolamento. In tal caso occorre sempre procedere alla anonimizzazione dei dati personali eventualmente presenti.

Nel caso in cui la legge od il regolamento preveda espressamente la pubblicazione di specifici documenti (ad esempio: curriculum vitae ex artt. 10 comma 8 lett. d; 14 comma 1 lett. b; 15 comma 1 lett. b; 26 comma 4; 27 comma 1 lett. f D.lgs. 33/2013), la struttura competente provvede a rendere non intellegibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili ai fini della trasparenza dell'azione amministrativa. A tal fine, ove possibile, le strutture predispongono una apposita modulistica per la raccolta dei soli dati personali necessari e pertinenti. A titolo di esempio il numero di telefono e l'indirizzo di

residenza/domicilio, pur raccolti per comunicare con l'interessato, non devono essere oggetto di pubblicazione in quanto non pertinenti per la finalità di trasparenza.

5.6. 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. 98 Codice). Con riferimento ai criteri generali per il trattamento dei dati personali l'art. 99 del Codice 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.

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 Codice.

5.6.1. 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" (art.101 Codice). I dati personali raccolti a tal fine non possono essere usati per adottare provvedimenti contro l'interessato, né per fini diversi. 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.

5.6.2. 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, nell'informativa di cui all'art.13 del Codice. 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.

5.6.2.1. 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 i principi di necessità e non eccedenza, in base ai quali 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, 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 che i responsabili del trattamento devono 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 Codice.

5.6.2.2. 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 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 competente in materia di statistica, 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.

5.6.2.3. 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 Codice, dal citato "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici", che 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 DPGR 12 febbraio 2013, n. 6/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.

5.6.2.4. Ricerca scientifica in ambito sanitario

Con riferimento alla ricerca scientifica in ambito sanitario, in aggiunta alle regole generali suddette, il quadro normativo si completa con l'art.110 del Codice, in base al quale 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, che non è necessario quando (art. 110 del Codice):

- 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 e sono trascorsi 45 gg. dalla comunicazione al Garante;
- non è possibile informare gli interessati, ma il progetto di ricerca ha ottenuto il parere favorevole del Comitato etico competente, ed è autorizzato dal Garante, anche con autorizzazione generale ai sensi dell'art. 40 del Codice.

6. RAPPORTI CON L'AUTORITA' 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 Regione - Giunta regionale, il quale vi provvede avvalendosi dell'Ufficio Privacy Regionale, che opera a supporto delle Direzioni generali, allo scopo di evitare frammentazioni.

7. ADEMPIMENTI

7.1. Notificazione al Garante .

Secondo quanto previsto dall'art.37 del Codice, 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 del trattamento.

7.2. Comunicazione al Garante

Secondo quanto previsto dall'art.39 comma 1 lett. a) del Codice, occorre effettuare una comunicazione al Garante quando il titolare Regione Toscana – Giunta Regionale, per lo svolgimento di funzioni istituzionali proprie del soggetto richiedente, deve comunicare ad altro soggetto pubblico dei dati personali ma ciò non sia previsto da norma di legge o di regolamento.

In questo caso, l'Ufficio Privacy Regionale invia la "comunicazione al Garante" e solo dopo che sono decorsi 45 giorni senza aver ricevuto diversa determinazione da parte del Garante stesso, si può dar luogo alla comunicazione dei dati richiesti al soggetto pubblico. Occorre tenere presente che il Garante può opporsi anche successivamente, interrompendo anche un flusso di dati eventualmente in corso.

7.3. 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 oralmente o per iscritto.

Ai sensi dell'art. 13 del Codice, l'informativa deve necessariamente contenere i seguenti elementi:

- 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 (vedi punto 8.4);
- la denominazione e la sede del titolare (Regione Toscana – Giunta Regionale) e del responsabile del trattamento, dandone indicazione non nominativa, ma facendo riferimento al dirigente della struttura regionale a ciò preposta.

Nelle strutture dove sono attivati sistemi di videosorveglianza finalizzati alla protezione dei dipendenti, 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) limitazione delle modalità di ripresa delle immagini (memorizzazione, 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) limitazione dei tempi di conservazione delle immagini (di regola fino a un massimo di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione ad attività particolarmente rischiose: in tali casi si possono conservare fino ad un massimo di 7 giorni);

c) individuazione dei soggetti legittimati ad accedere alle registrazioni;

d) indicazione del soggetto e della struttura cui l'interessato può rivolgersi e dei diritti che può esercitare.

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:

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 eventuali sanzioni amministrative 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 (amministratori e organi istituzionali di enti controllati, 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;

• Consulenti, liberi professionisti (contratti, convenzioni, incarichi professionali): l'informativa preferibilmente deve essere inserita 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 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 dai Responsabili del trattamento, con il supporto dell'Ufficio Privacy e possono essere redatte sulla base dei modelli consultabili nel sito Intranet regionale dedicato all'area tematica "Privacy".

7.4. Diritti dell'interessato

Le strutture 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 punto 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 in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

7.4.1. Esercizio dei diritti dell'interessato

L'interessato può esercitare i suoi diritti rivolgendosi al titolare o al responsabile del trattamento, con una richiesta anche non formale, che non può essere rinnovata, salvo giustificati motivi, prima di novanta giorni (così dispone l'art. 9 comma 5 del Codice).

Per l'esercizio dei diritti dell'interessato il Garante ha predisposto un fac-simile di modulo, scaricabile dal suo sito web o reperibile presso URP della Regione Toscana o presso l'Ufficio Privacy.

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. Se richiesto, 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

La legge regionale 23 luglio 2009, n.40 "Legge di semplificazione e riordino normativo 2009", in attuazione al dettato statutario ed al principio di massima trasparenza e pubblicità dell'azione amministrativa, al Titolo II – Capo I – Sezione I detta disposizioni specifiche in merito all'accesso agli atti amministrativi dell'amministrazione regionale, riconoscendo il diritto di accesso ai documenti amministrativi a chiunque senza obbligo di motivazione, ad eccezione dei documenti contenenti dati personali, per i quali si continuano ad applicare le disposizioni previste dalla L.241/90.

L'istanza di accesso a documenti contenenti dati personali deve pertanto essere motivata da un interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento per il quale è richiesto l'accesso.

Il diritto di accesso previsto dalla L.241/90:

- assicura la trasparenza dell'attività amministrativa
- riguarda il documento amministrativo
- prevale quando c'è un interesse per la tutela di situazioni giuridicamente rilevanti.

Il diritto alla riservatezza previsto dal Codice Privacy:

- garantisce il rispetto dei diritti, delle libertà fondamentali e della dignità dell'individuo
- riguarda il dato personale
- recede nel caso in cui si debba garantire l'accesso per la tutela di situazioni giuridicamente rilevanti.

Entrambi i diritti sono costituzionalmente garantiti e sono solo apparentemente in antitesi, in quanto la normativa in materia di protezione dei dati personali si pone come fattore delimitativo, sotto il profilo delle modalità tecniche di esercizio, ma non preclusivo dell'esercizio dell'accesso.

L'articolo 59 del Codice stabilisce che i presupposti, le modalità e i limiti del diritto di accesso restano disciplinati dalla Legge 241/90 e che tali norme si considerano di rilevante interesse pubblico. Si afferma pertanto che l'accesso è la regola dell'azione amministrativa e la tutela della riservatezza è l'eccezione alla regola.

La disciplina da applicare si distingue in base al tipo di dati personali contenuti nel documento oggetto della richiesta di accesso:

- documento contenente dati comuni: si applicano gli artt. 22 (principi per l'accesso) e 24 (esclusione dell'accesso) della L.241/90;
- documento contenente dati sensibili e giudiziari: si applica l'art. 24 comma 7 della L. 241/90 in base al quale l'accesso consentito nei limiti in cui sia strettamente indispensabile (principio di necessità e non eccedenza) per curare o difendere i propri interessi giuridici. La richiesta di accesso deve contenere la motivazione della indispensabilità;
- documento contenente "dati supersensibili" (relativi allo stato di salute e alla vita sessuale) si applica l'art. 60 del Codice in base al quale "il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile". Questo pone in capo alla PA l'onere di un doppio giudizio discrezionale relativo sia all'indispensabilità dell'accesso che alla comparazione degli interessi da tutelare. In questa valutazione l'amministrazione è aiutata dalla casistica redatta dal Garante (es. Dati sanitari - Provvedimento generale sui diritti di pari rango del 09.03.2003). Il Garante ha stabilito che nel valutare il "rango" del diritto di un terzo si deve utilizzare come parametro di raffronto non il "diritto di azione e difesa", che pure è costituzionalmente garantito, quanto il diritto sottostante che il terzo intende tutelare in giudizio sulla base del documento che chiede di conoscere.

8.1.1. Diritto di accesso dei consiglieri regionali

Lo Statuto della Regione Toscana all'art. 9 co. 2 recita " ogni consigliere ha diritto, per l'espletamento del mandato, di accedere agli uffici della Regione e di ottenere la documentazione e le informazioni in loro possesso, nel rispetto delle norme a tutela della riservatezza e con obbligo di osservare il segreto nei casi previsti dalla legge".

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 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.

Quando la richiesta di accesso ha ad oggetto dati inerenti lo stato di salute occorre che dalla stessa si evinca l'indispensabilità dei dati ai fini dell'espletamento della funzione rivestita, evitando così un ingiustificato pregiudizio alla riservatezza degli interessati.

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 1.

In particolare devono:

- a) assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati a trattarle;

- 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.

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 backup;
- 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;
- adozione di tecniche di cifratura o codici identificativi per dati sensibili, trattati con strumenti elettronici.

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 1, 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, che 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)

9.1. Sicurezza degli archivi cartacei

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 incaricati 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

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 custodite con le stesse modalità dei documenti originali e anche la loro distruzione deve avvenire 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:

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

9.2. Accesso ai dati sensibili e giudiziari

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, 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.

9.3. Adempimenti relativi ai fornitori che possono venire a conoscenza di dati personali

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 annuale per la sicurezza dei dati personali-

Nel caso di trattamenti di dati personali il Codice prevede che debbano essere adottate idonee misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31).

Ai trattamenti devono inoltre essere applicate le misure minime di sicurezza, indicate dagli artt. 33 – 35 del Codice e dettagliate nel Disciplinare Tecnico del Codice.

Il dirigente competente in materia di privacy, sentiti i dirigenti competenti in materia di sicurezza informatica, sistemi informativi e sicurezza delle sedi regionali, adotta annualmente il "Documento Annuale per la Sicurezza dei dati personali", in cui dà atto dell'adozione di tali misure.

Il DAS deve pertanto:

- identificare e classificare le informazioni ed i dati personali trattati dalle strutture della Giunta regionale;
- contenere l'elenco dei ruoli e delle responsabilità all'interno dell'amministrazione regionale;
- identificare i luoghi fisici ove vengono custodite e trattate le informazioni e i dati personali;
- identificare le risorse software ed hardware con cui vengono trattate e custodite le informazioni e i dati personali;
- analizzare i rischi cui possono essere esposti dati e informazioni;
- individuare le misure di sicurezza adottate per i diversi ambienti/archivi sia informatici che cartacei;
- individuare i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza;
- individuare le procedure per il controllo dell'accesso delle persone autorizzate ai locali interessati dalle misure di sicurezza;
- individuare i criteri e le modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- contenere l'elenco dei trattamenti affidati all'esterno

Ciascun responsabile di trattamento è tenuto ad applicare le misure di sicurezza previste nel Documento annuale per la Sicurezza dei dati per quanto di propria competenza, sulla base delle responsabilità individuate nel Documento stesso.

PARTE III^

ALLEGATO 1

“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. Quando i documenti riservati sono conservati in armadi a vetri è sempre meglio oscurarli, apponendo alle ante fogli di carta montati all'interno.

2. CONSERVATE I SUPPORTI ESTRAIBILI (CDROM, 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
- La password di accesso alla rete Novell impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
- La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
- 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.
- la password per l'accesso alla posta elettronica e/o agenda impedisce l'eventuale accesso non autorizzato alla visualizzazione della posta e degli appuntamenti

4. COME DEVE ESSERE SCELTA LA PASSWORD

La parola chiave per l'accesso alla rete Novell ed alla posta elettronica deve essere lunga almeno 8 caratteri, avere almeno una lettera maiuscola, almeno un numero, può contenere caratteri speciali e non può terminare con un numero.

In generale ogni parola chiave non deve contenere caratteri riconducibili ad informazioni personali e/o di lavoro (ad esempio matricola, data di nascita) dell'incaricato ed deve essere modificata al primo utilizzo e successivamente ogni sei mesi.

L'amministrazione, ove necessario, adotterà ulteriori meccanismi di obbligo del cambio password con le modalità ritenute opportune od imposte dalla legge.

5. 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.

e) 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.

f) custodite le password in un luogo sicuro

6. 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.

Distrugete personalmente le stampe quando non servono più.

Se una stampante si blocca, assicuratevi, eventualmente coinvolgendo il personale ASTI (Assistenza Servizi Telematici e Informatici), che non restino dati importanti o riservati nella memoria della stampante, che potrebbero essere di nuovo inviati in stampa una volta che le funzionalità della stampante sono state ripristinate.

7. NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file dal pc, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati, per essere sicuri di averli rimossi, dopo la cancellazione occorre effettuare un defrag (compattazione) del disco. E' comunque sempre consigliabile conservare i dati sensibili sul disco di rete dove i dati sono backuppati automaticamente e resi visibili/modificabili solo a chi è autorizzato.

8. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i ladri, anche fuori dalla sede di lavoro. Se avete necessità di gestire dati riservati utilizzate sempre e solo il disco di rete.

9. 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.

10. 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 vostro dirigente ed eventualmente inviate una specifica richiesta al settore competente.

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

I vostri dati dovrebbero 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, chiavi usb etc.)

12. 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;
3. Attraverso supporti esterni (ad esempio chiavi usb) contenenti file non controllati da antivirus.
4. attraverso mail anche non contenente allegati (potrebbe infatti contenere un link che aprendolo attiva anche il virus)

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da chiavette USB;
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;

4. Diffusione del virus su altre stazioni collegate al network aziendale.

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 supporto estraibile

Infatti se il supporto estraibile fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.

3. 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. Attualmente esiste una consolle centralizzata della McAfee che provvede a segnalare al presidio di assistenza delle postazioni di lavoro le macchine che non sono aggiornate.

COME EVITARE DI DIFFONDERE I VIRUS:

4. 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).

5. 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.

13. POSTA ELETTRONICA/INTERNET

L'uso della Posta elettronica e di Internet deve essere improntato a quanto previsto nell'apposito disciplinare per l'utilizzo degli strumenti informatici, della rete telematica e del sistema di telefonia fissa e mobile all'interno della Giunta Regionale Toscana, che dispone in merito alle corrette modalità di utilizzo di tali strumenti informatici da parte dei dipendenti regionali per lo svolgimento delle mansioni loro attribuite. Tale atto è reperibile nella intranet regionale, alla sezione privacy.

ALLEGATO 2

SISTEMA PRIVACY

Il processo trasversale "Sistema privacy" è l'insieme di procedure, attività e relazioni che attengono la protezione dei dati personali (D.Lgs. 196/2003), e che coinvolgono la Regione Toscana, sia nei propri rapporti interni, sia nei rapporti che intercorrono con il sistema degli Enti, delle Agenzie, e con altri soggetti della P.A. (per materie delegate dalla Regione stessa).

I soggetti principalmente coinvolti nelle procedure organizzative che sono descritte di seguito sono l'Ufficio Privacy Regionale e il Referente del "sistema privacy" presso le direzioni generali. Ufficio Privacy Regionale

Codifica	Processo	Nome procedura
Privacy - 1	Sistema Privacy	Predisposizione regolamento sui dati sensibili e giudiziari

OBIETTIVO

La presente procedura definisce le responsabilità e le modalità per la predisposizione del regolamento sui dati sensibili e giudiziari.

NOTA

La procedura ha la finalità di organizzare il rapporto che intercorre fra l'Ufficio Privacy regionale ed il referente del sistema privacy presso le Direzioni generali.

RIFERIMENTI NORMATIVI

D.Lgs. 196/2003 articoli 20 e 21

LEGENDA DELLE STRUTTURE COINVOLTE NELLA PROCEDURA

UPR: Struttura competente in materia di protezione dei dati personali (Ufficio Privacy regionale)

RSP: Referente del "Sistema privacy" presso le Direzioni Generali

RT: Responsabile del trattamento

CTD: Comitato tecnico di direzione

GR: Giunta regionale

MATRICE DI SINTESI DELLE RESPONSABILITÀ

ATTIVITA'	RESPONSABILITA'	UPR	RT/ RSP	CTD	GR
1 - Individuazione e segnalazione all'UPR dei trattamenti soggetti a regolamento			X		
2 - Consulenza, supporto e verifica delle segnalazioni delle DG		X			
3 - Predisposizione bozza schema tipo regolamento		X			
4 - Richiesta parere di conformità al Garante		X			
5 - Integrazione schema tipo regolamento con legislazione regionale		X	X		
6 - Inoltro al CTD della proposta di regolamento		X			
7 - Presa visione della proposta di regolamento				X	
8 - Approvazione regolamento					X

DESCRIZIONE DELLE ATTIVITÀ

Attività	Descrizione	Modulistica/ procedure	Scadenze
1	Il RSP individua e segnala all'UPR i trattamenti soggetti a regolamento		
2	L'UPR fornisce consulenza e supporto ai RT/RSP in merito all'individuazione dei trattamenti soggetti a regolamento e verifica tutte le segnalazioni		
3	L'UPR predispose la bozza di regolamento*		
4	L'UPR richiede al Garante il parere di conformità sulla bozza di regolamento**		
5	L'UPR richiede ai RT/RSP di integrare lo schema tipo di regolamento con la legislazione regionale		
6	L'UPR inoltra al CTD la proposta di regolamento definitiva		
7	Il CTD prende visione della proposta di regolamento		
8	La GR adotta il regolamento con proprio atto		

* La predisposizione della bozza di regolamento avviene su schema-tipo in sede di Gruppo di lavoro interregionale cui partecipano i rappresentanti di tutte le Regioni

** Il Garante esprime il parere sullo schema tipo; se ci sono osservazioni da parte del Garante il flusso ricomincia dall'attività n.3.

NOTA:

La procedura organizzativa disegnata viene seguita anche per gli aggiornamenti del regolamento .

Codifica	Processo	Nome procedura
Privacy – 2	Sistema Privacy	Notificazione al Garante

OBIETTIVO

La presente procedura definisce le responsabilità e le modalità per la predisposizione e l'inoltro della notificazione al Garante della privacy.

NOTA

La procedura ha la finalità di organizzare il rapporto che intercorre fra l'Ufficio Privacy regionale ed il referente del sistema privacy presso le Direzioni generali.

RIFERIMENTI NORMATIVI

D.Lgs. 196/2003 articoli 37 e 38

LEGENDA DELLE STRUTTURE COINVOLTE NELLA PROCEDURA

UPR: Struttura competente in materia di protezione dei dati personali (Ufficio Privacy regionale)

RSP: Referente del "Sistema privacy" presso le Direzioni Generali

RT: Responsabile del trattamento

DGOR: Direttore generale competente in materia di organizzazione e risorse

MATRICE DI SINTESI DELLE RESPONSABILITÀ

ATTIVITA'	RESPONSABILITA'	UPR	RT/ RSP	DGOR
1 – Rilevazione dei casi in cui può sussistere la necessità di notifica dei trattamenti			X	
2 – Supporto e consulenza alle strutture regionali		X		
3 – Espletamento istruttoria e redazione notificazione		X		
4 – Invio testo notificazione al DGO		X		
5 – Inoltro notificazione al Garante				X

DESCRIZIONE DELLE ATTIVITÀ

Attività	Descrizione	Modulistica/ procedure	Scadenze
1	Il RSP collabora con i RT nell'individuazione e nella segnalazione all'UPR dei trattamenti oggetto di notificazione al Garante		
2	L'UPR fornisce consulenza e supporto in materia di notificazione al Garante e valuta la necessità di procedere alla notifica dei trattamenti al Garante		
3	L'UPR cura l'istruttoria del materiale inviato dal RSP di ciascuna DG e redige la notificazione		
4	L'UPR invia il testo della notificazione al DGO		
5	Il DGO inoltra la notificazione al Garante per via telematica con firma digitale	Modello telematico predisposto dal Garante	Prima dell'inizio del/dei trattamento/i

Codifica	Processo	Nome procedura
Privacy – 3	Sistema Privacy	Documento Annuale per la sicurezza dei dati

OBIETTIVO

La presente procedura definisce le responsabilità e le modalità per la predisposizione dell'aggiornamento del documento annuale per la sicurezza dei dati (DAS).

NOTA

La procedura ha la finalità di organizzare il rapporto che intercorre fra l'Ufficio Privacy regionale ed il referente del sistema privacy presso le Direzioni generali.

RIFERIMENTI NORMATIVI

D.Lgs. 196/2003 e DGR 388 del 14.05.2012

LEGENDA DELLE STRUTTURE COINVOLTE NELLA PROCEDURA

UPR: Struttura competente in materia di protezione dei dati personali (Ufficio Privacy regionale)

RSP: Referente del "Sistema privacy" presso le Direzioni Generali

RT: Responsabile del trattamento

SSR: struttura competente in materia di sicurezza sedi regionali

SIN: Struttura competente in materia di sicurezza informatica

SINF: struttura competente in materia di sistemi informativi

RUPR: dirigente responsabile in materia di privacy

MATRICE DI SINTESI DELLE RESPONSABILITÀ

ATTIVITA'	RESPONSABILITA'	UPR	RT/ RSP/	SIN/ SINF /SSR	RUPR	GR
1 – rilevazione delle misure di sicurezza adottate		X	X	X		
2 – Redazione DAS		X		X		
6 – Approvazione del DAS					X	

DESCRIZIONE DELLE ATTIVITÀ

Attività	Descrizione	Modulistica/ procedure	Scadenze
1	L'UPR in collaborazione con RT, RSP e SIN/SINF/SSR effettua la rilevazione delle misure di sicurezza adottate		
2	L'UPR, sentite le strutture interessate, e in collaborazione con SIN/SINF/SSR redige il DAS aggiornato		
3	Il RUPR approva l'aggiornamento del DAS		Entro l'anno solare

Codifica	Processo	Nome procedura
Privacy – 4	Sistema Privacy	Comunicazione al Garante

OBIETTIVO

La presente procedura definisce le responsabilità e le modalità per la comunicazione al Garante relativa alla trasmissione di dati comuni a soggetti pubblici in assenza di previsione normativa.

NOTA

La procedura ha la finalità di organizzare il rapporto che intercorre fra l'Ufficio Privacy regionale ed il referente del sistema privacy presso le Direzioni generali.

RIFERIMENTI NORMATIVI

D.Lgs. 196/2003 articolo 39

LEGENDA DELLE STRUTTURE COINVOLTE NELLA PROCEDURA

UPR: Struttura competente in materia di protezione dei dati personali (Ufficio Privacy regionale)

RSP: Referente del "Sistema privacy" presso le Direzioni Generali

RT: Responsabile del trattamento

MATRICE DI SINTESI DELLE RESPONSABILITÀ

ATTIVITA'	RESPONSABILITA'	UPR	RSP	RT
1 – Segnalazione richiesta dati comuni da soggetti pubblici				X
2 – Verifica previsione normativa relativa alla trasmissione dati			X	
3 – Segnalazione assenza della previsione normativa e richiesta di darne comunicazione al Garante				X
4 – Richiesta autorizzazione al Garante per trasmissione dati al richiedente		X		
5 – Segnalazione esito comunicazione al Garante		X		

DESCRIZIONE DELLE ATTIVITÀ

Attività	Descrizione	Modulistica/ procedure	Scadenze
1	Il RT segnala al RSP la richiesta di dati comuni da parte di soggetti pubblici		
2	Il RSP verifica se la trasmissione dei dati richiesti è prevista da legge o da regolamento		
3	Se non è prevista il RT, segnala il caso all'UPR perché ne dia comunicazione al Garante		
4	L'UPR richiede al Garante l'autorizzazione a trasmettere i dati al soggetto richiedente		
5	L'UPR segnala al RSP l'esito della comunicazione al Garante		Il Garante si esprime entro 45 gg dalla ricezione della comunicazione *

*Scaduti i 45 gg. I dati possono essere trasmessi al richiedente anche in assenza di indicazione del Garante.

Codifica	Processo	Nome procedura
Privacy – 5	Sistema Privacy	Aggiornamento Archivio TDP

OBIETTIVO

La presente procedura definisce le responsabilità e le modalità per l'aggiornamento dell'Archivio dei trattamenti TDP.

NOTA

La procedura ha la finalità di organizzare il rapporto che intercorre fra l'Ufficio Privacy regionale ed il referente del sistema privacy presso le Direzioni generali.

RIFERIMENTI NORMATIVI

D.Lgs. 196/2003 Allegato B

LEGENDA DELLE STRUTTURE COINVOLTE NELLA PROCEDURA

UPR: Struttura competente in materia di protezione dei dati personali (Ufficio Privacy regionale)

RSP: Referente del "Sistema privacy" presso le Direzioni Generali

RT: Responsabile del trattamento

DG: Direttori generali

MATRICE DI SINTESI DELLE RESPONSABILITÀ

ATTIVITA'	RESPONSABILITA'	UPR	RSP	RT	DG
1 – Adozione del decreto di assegnazione nuovi incarichi dirigenziali con la nomina dei responsabili del trattamento					X
2 – Definizione istruzioni e criteri per l'aggiornamento dell'archivio dei trattamenti		X			
3 – Supporto ai RT			X		
4 – Aggiornamento archivio e stampa OdS tramite procedura Informatica (TDP)				X	
5 – trasmissione ODS agli uffici competenti				X	
6 – Monitoraggio dei trattamenti di competenza della DG		X	X		
7 – verifica della coerenza dei trattamenti censiti in TDP		X			

DESCRIZIONE DELLE ATTIVITÀ

Attività	Descrizione	Modulistica/ procedure	Scadenze
1	Il DG adotta il decreto di assegnazione nuovi incarichi dirigenziali con la nomina dei responsabili del trattamento		
2	L'UPR definisce le istruzioni e i criteri per l'aggiornamento dell'archivio dei trattamenti		
3	Il RSP supporta i responsabili dei trattamenti nell'aggiornamento degli archivi		
4	Il RT aggiorna i trattamenti di sua competenza e fa gli		Cadenza annuale

	ODS per i suoi incaricati		
5	Il RSP svolge funzioni di monitoraggio dei trattamenti di competenza della DG		
6	L'UPR verifica la coerenza dei trattamenti censiti in TDP		