ARS TOSCANA
agenzia regionale di sanità

DECRETO DEL DIRETTORE

n. 48 del 16/09/2014

Oggetto: **Decreto legislativo 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*) – Ex artt. 28 e 29 - Nomina dei Responsabili trattamento dati personali e istruzioni del titolare ai responsabili**

IL DIRETTORE

Vista la legge regionale 24 febbraio 2005, n. 40 (*Disciplina del servizio sanitario regionale*) e successive modifiche ed integrazioni;

Visto il decreto del Presidente della Giunta Regionale n. 167 del 12 ottobre 2011, con il quale il sottoscritto è stato nominato Direttore dell'ARS;

Visto il Regolamento generale di organizzazione dell'ARS, approvato dalla Giunta regionale con deliberazione n. 29 del 21.01.2008;

Visto il decreto legislativo 30 giugno 2003 *(Codice in materia di protezione di dati personali),* di seguito denominato "Codice";

Richiamati, in particolare, l'art. 16, dir. 95/46/CE e gli articoli 28, 29 e 30 del citato Codice che disciplinano le figure del titolare, del responsabile e degli incaricati del trattamento dei dati personali, definendone compiti e responsabilità;

Considerato che l'ARS nel suo complesso è il titolare del trattamento dei dati personali ed esercita un potere decisionale del tutto autonomo sulle finalità e le modalità del trattamento, ivi compreso il profilo della sicurezza, tramite il suo direttore, in qualità di rappresentante legale dell'Ente;

Vista la legge regionale 24 febbraio 2005, n. 40 (*Disciplina del servizio sanitario regionale*) e successive modificazioni ed integrazioni e specificatamente:

a) l'art. *82* septies comma 1, lett. a), che attribuisce al Direttore dell'ARS la rappresentanza legale dell'Ente;
b) gli artt. 82 novies e 82 decies relativamente ai compiti ed alla nomina del Direttore;
c) l'art. 82 novies decies relativamente alle attività svolte dalle strutture tecnico scientifiche e in particolare il comma 2 che individua nei responsabili delle strutture scientifiche, i responsabili del trattamento dei dati sensibili a livello individuale, nominativo o comunque identificabile;

Ritenuto di dover procedere, in un'ottica di semplificazione, ad una revisione degli atti dell'Agenzia sopra richiamati al fine di:

- recepire le modifiche legislative che hanno interessato in questi anni il d.lgs n. 196/2003 e le novità introdotte dagli altri provvedimenti del Garante che hanno innovato ed integrato le disposizioni in materia di tutela della privacy;
- ricondurre tutta la disciplina regionale in materia di privacy ad un unico atto organico, che costituisca uno strumento operativo a disposizione delle strutture di ARS che assumono ruoli di responsabilità nel trattamento dei dati personali (dipendenti addetti al trattamento di dati personali, Dirigenti responsabili del trattamento, collaboratori esterni, etc.);

- aggiornare la disciplina della privacy tenuto conto del mutato assetto organizzativo dell'Agenzia, intervenuto a varie riprese con la revisione della legge istitutiva;

Considerata altresì la necessità di revocare la deliberazione del Consiglio di Amministrazione n. 18 del 28.06.2004 e ss.mm. e, alla luce della nuova situazione normativa, di approvare le nuove nomine ed istruzioni per i responsabili dei trattamenti per l'attuazione del "*Codice in materia di protezione dei dati personali*"; nonché le successive deliberazioni di modifiche ed integrazioni, in particolare:- la precedente deliberazione del Consiglio di Amministrazione n.. 17 del 19/03/2008 recante "*Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) – Ex artt. 28 e 29 - Nomina dei Responsabili trattamento dati personali –Approvazione testo coordinato con le disposizioni di cui alle deliberazione del consiglio di amministrazione n. 18 del 28/06/2004, n. 5 del 13/04/2005, n. 12 del 16/04/2007 e n. 5 del 31/01/2008*."

Considerato necessario procedere alla nomina dei responsabili del trattamento dei dati personali degli Osservatori di Epidemiologia e per la Qualità e l'Equità, individuandoli nei due Coordinatori, così come previsto dall'articolo 82 *duodecies*, comma 2, della l.r. n. 40/2005 e ss.mm.;

Valutata l'urgenza che i Coordinatori degli Osservatori provvedano alla designazione degli incaricati del trattamento, ciascuno per la struttura diretta, definendo l'ambito di competenza ed impartendo le prescrizioni tecniche, ivi compreso il profilo relativo alla sicurezza, cui i medesimi incaricati devono attenersi, secondo il disposto dell'art. 30 del più volte richiamato "Codice";

Ritenuto opportuno impartire, in ossequio alla disciplina recata dal d.lgs. n. 196/2003 e ss.mm., le istruzioni di cui all'allegato 1, parte integrante e sostanziale del presente atto, contenente una dettagliata descrizione analitica dei compiti affidati ai responsabili del trattamento, ivi compreso il profilo di sicurezza, secondo il disposto dell'ordinamento statale e regionale vigente;

Valutato necessario che i responsabili interni si impegnino, in particolare, a:

a) trattare i dati personali che verranno loro comunicati da ARS per le sole finalità connesse allo svolgimento delle attività previste da convenzione o contratto, in modo lecito e secondo correttezza;
b) nominare con nota scritta, protocollata e con data certa gli incaricati del trattamento, fornendo loro le necessarie istruzioni;
c) garantire la riservatezza di tutte le informazioni che verranno loro trasmesse, impedendone l'accesso a chiunque, con la sola eccezione del proprio personale, espressamente nominato incaricato al trattamento e a non portare a conoscenza di terzi, per nessuna ragione ed in nessun momento, presente o futuro, le notizie ed i dati pervenuti a loro conoscenza, se non previa espressa autorizzazione scritta di ARS;
d) consentire al personale autorizzato da ARS di effettuare controlli sul rispetto delle istruzioni impartite, nonché delle misure di sicurezza adottate previo accordo tra le parti;

Ritenuto che, per il raggiungimento degli scopi indicati, al capoverso che precede, i predetti responsabili debbano adottare:

a) idonee e preventive misure di sicurezza atte ad eliminare o, comunque, a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell'art. 31 del d.lgs n. n. 196/2003 e ss.mm.;
b) tutte le misure di sicurezza, previste dagli articoli 33, 34, 35, 36, del d.lgs n. 196/2003 e ss.mm., che configurano il livello minimo di protezione richiesto in relazione ai rischi di cui all'articolo 31, analiticamente specificate nell'Allegato B al decreto stesso, denominato "Disciplinare tecnico in materia di misure di sicurezza";

Ritenuto opportuno istituire, per il combinato disposto degli artt. 34 e 180 del "Codice", il censimento dei dati personali, suddiviso per tipologie e per strutture organizzative, denominato (CE.TRA.), di cui al cap. 9 dell'allegato 1, al presente atto;

Valutato altresì necessario, rendere permanente un gruppo di lavoro denominato "Gruppo Privacy", stante l'impatto trasversale del "Codice" che richiede una serie di adempimenti, a rilevanza interna ed esterna, la cui attuazione implica un'approfondita attività di monitoraggio, attraverso il coinvolgimento di più soggetti, con competenze e formazione diversificati;

Ritenuto che per la composizione del Gruppo Privacy e per i relativi compiti si fa espresso rinvio a quanto disciplinato al cap. 10 dell'allegato 1 al presente atto e che la nomina sia attuata mediante decreto del direttore, adottato sulla base delle designazioni dei rispettivi responsabili di struttura e settori individuati;

DECRETA

1) di stabilire che l'ARS nel suo complesso è il titolare del trattamento dei dati personali dell'Agenzia e che la stessa esercita un potere decisionale del tutto autonomo sulle finalità e le modalità del trattamento, ivi compreso il profilo della sicurezza, tramite il suo Direttore, in qualità di rappresentante legale dell'Ente;

2) di nominare, per le motivazioni esposte in narrativa e secondo il disposto dell'ordinamento statale e regionale vigente in materia, responsabili del trattamento dei dati personali dell'ARS, i sotto elencati soggetti, definendo a fianco di ciascuno l'ambito di competenza:

a) Fabio Voller (f.f. coordinatore Osservatorio di Epidemiologia)	Responsabile del trattamento di dati personali dell'Osservatorio di Epidemiologia;
b) Andrea Vannucci (coordinatore Osservatorio per la Qualità e l'Equità)	Responsabile del trattamento dei dati personali dell'Osservatorio per la Qualità e l'Equità;

3) di approvare secondo il disposto dell'art. 29 del d.lgs. 196/2003 le istruzioni, ivi compreso il profilo di sicurezza, contenute nell'allegato 1, parte integrante e sostanziale del presente atto, da impartire ai responsabili di cui al punto 2;

4) di stabilire che i responsabili esterni si impegnino in particolare a:
   a) trattare i dati personali che verranno loro comunicati da ARS per le sole finalità connesse allo svolgimento delle attività previste da convenzione o contratto, in modo lecito e secondo correttezza;
   b) nominare per iscritto gli incaricati del trattamento, fornendo loro le necessarie istruzioni;
   c) garantire la riservatezza di tutte le informazioni che verranno loro trasmesse, impedendone l'accesso a chiunque, con la sola eccezione del proprio personale, espressamente nominato incaricato al trattamento e a non portare a conoscenza di terzi, per nessuna ragione ed in nessun momento, presente o futuro, le notizie ed i dati pervenuti a loro conoscenza, se non previa espressa autorizzazione scritta di ARS;
   d) consentire al personale autorizzato da ARS di effettuare controlli sul rispetto delle istruzioni impartite, nonché delle misure di sicurezza adottate previo accordo tra le parti;

5) di disporre che i responsabili interni debbano, altresì, adottare:
   a) idonee e preventive misure di sicurezza atte ad eliminare o, comunque, a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell'art. 31 del d.lgs. n. 196/2003 e ss.mm.;

b) tutte le misure di sicurezza, previste dagli articoli 33, 34, 35, 36, del d.lgs. n. 196/2003, che configurano il livello minimo di protezione richiesto in relazione ai rischi di cui all'articolo 31, analiticamente specificate nell'Allegato B al decreto stesso, denominato "Disciplinare tecnico in materia di misure di sicurezza";

6) di disporre che i responsabili del trattamento procedano celermente alla designazione degli incaricati del trattamento, con nota scritta protocollata e avente data certa, impartendo loro le relative istruzioni, ivi compreso il profilo di sicurezza. Per gli incaricati designati dal *Direttore* le istruzioni sono definite di concerto con gli altri Coordinatori, essendo riferite a strutture trasversali per gli osservatori e incidendo su trattamenti afferenti ad entrambi gli osservatori;

7) di istituire, per il combinato disposto degli artt. 34 e 180 del "Codice", il censimento dei dati personali, suddiviso per tipologie e per strutture organizzative, denominato (CE.TRA.), secondo le indicazioni di cui al cap. 9 dell'allegato 1, al presente atto;

8) di rendere permanente per le motivazioni espresse in premessa, un gruppo di lavoro denominato "Gruppo Privacy", per la cui composizione e relativi compiti si fa espresso rinvio a quanto disciplinato al cap. 10 dell'allegato 1 al presente atto, disponendo altresì che la nomina sia attuata mediante decreto del Direttore adottato sulla base delle designazioni dei rispettivi responsabili di struttura e settori individuati nel citato allegato 1;

9) di revocare, per i motivi espressi in narrativa, la deliberazione del Consiglio di Amministrazione n. 18 del 28.06.2004 e ss.mm. e, alla luce della nuova situazione normativa, di approvare le nuove nomine ed istruzioni per i responsabili dei trattamenti per l'attuazione del "Codice in materia di protezione dei dati personali"; nonché le successive deliberazioni di modifiche ed integrazioni, in particolare:- la precedente deliberazione del Consiglio di Amministrazione n.. 17 del 19/03/2008 recante "*Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) – Ex artt. 28 e 29 - Nomina dei Responsabili trattamento dati personali –Approvazione testo coordinato con le disposizioni di cui alle deliberazione del consiglio di amministrazione n. 18 del 28/06/2004, n. 5 del 13/04/2005, n. 12 del 16/04/2007 e n. 5 del 31/01/2008.*"

10) di assicurare la pubblicità integrale del presente provvedimento mediante inserimento nella sezione "*Amministrazione trasparente*" sul sito web dell'ARS (www.ars.toscana.it).

Il Direttore
Dott. Francesco Cipriani

ARS TOSCANA
agenzia regionale di sanità

Allegato n. 1
al decreto direttore n. 48 del 16/09/2014

TRATTAMENTO DATI SENSIBILI
ISTRUZIONI
DEL TITOLARE DEL TRATTAMENTO

INTRODUZIONE

Con l'entrata in vigore il 1° gennaio 2004 del nuovo "Codice" in materia di protezione di dati personali (Dlgs. 30 Giugno 2003, n. 196), di seguito denominato "Codice" o decreto, il cammino iniziato già diversi anni fa con la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, ratificata con legge 4 agosto 1955, n. 848, con le direttive del Parlamento Europeo e del Consiglio dell'Unione europea e, tra queste, la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, recepita nel nostro Paese dalla legge 675/1996, trova oggi un nuovo impulso, nell'ottica della definizione di regole sostanziali più che formali, anche per effetto del recepimento nel nuovo "Codice" della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002.

L'Agenzia Regionale di Sanità, che per finalità istitutive è preposta al trattamento di dati sensibili, in ossequio ai principi sanciti dalla Comunità Europea e dal legislatore statale, intende procedere alla definizione di un sistema di tutela della privacy, nella convinzione che attraverso il rispetto dei dati della persona si può ottenere un risultato importante: quello della tutela della dignità dei cittadini.

Nell'ottica predetta, s'impone pertanto un impegno organizzativo che passerà attraverso azioni successive a breve, medio termine sino a giungere, in armonia con le scadenze dettate dal nuovo "Codice", alla definizione di un sistema di regole certe.

Si delineano, di seguito, i passaggi fondamentali di detto impegno:

1. *AZIONI A BREVE TERMINE*

- Aggiornamento della nomina dei Responsabili del trattamento dei dati sensibili (cfr. art 16, dir. 95/46/CE; art. 8, comma 1; artt. 28 e 29 del "Codice"), tenuto conto del rinnovato assetto organizzativo;
- Affidamento compiti dal Titolare al Responsabile (comma 4) e definizione delle istruzioni, ivi compreso il profilo della sicurezza, (cfr. art 16, dir. 95/46/CE; art. 8, comma 1; art. 29 del "Codice");
- Designazione degli incaricati del trattamento da parte dei o del titolare o Responsabili (cfr. art 17, par. 3, dir. 95/46/CE; art. 8, comma 5, e 19; art. 30 del "Codice"); individuazione dell'ambito di trattamento loro consentito (art. 30, co. 2) *"si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato per iscritto l'ambito del trattamento consentito agli addetti dell'unità medesima"*.
- Elaborazione delle istruzioni, ivi compreso il profilo della sicurezza, da parte dei responsabili del trattamento, da impartire agli incaricati del trattamento stesso, cui i medesimi devono attenersi (cfr. art 17, par. 3, dir. 95/46/CE; art.8, comma 5, e 19; art. 30 del "Codice");

2. *AZIONI A MEDIO TERMINE*

- In occasione dell'aggiornamento, introduzione, all'interno del Regolamento di Organizzazione dell'ARS, ex art. 82 *terdecies* legge regionale 24 febbraio 2005 n. 40 "*Disciplina del Servizio sanitario regionale*." e successive modificazioni, di seguito denominata legge regionale, dei principi generali in tema di "Trattamento dati sensibili";
- Adozione, entro il 31 ottobre 2014, di un protocollo operativo che individui le casistiche principali in cui opera ARS, i dati trattabili e le operazioni eseguibili ove, per effetto dello sviluppo delle attività dell'ARS, l'esigenza di ricerca vada oltre i dati specificati dalla legge istitutiva (art. 20, comma 2, e art. 181, d.lgs. 196/2003).

L'intento è anche quello di permettere a tutti gli addetti di operare nel quadro d'indicazioni certe, che non devono essere intese come ulteriore appesantimento burocratico, ma come miglioramento della qualità del servizio offerto ai cittadini.

Il presente documento, che contiene le indicazioni del Titolare da impartire ai Responsabili del trattamento, si colloca nell'ambito delle azioni a breve termine sopra enunciate, ed ha lo scopo di

avviare il processo di regolazione della materia. Le stesse sono impartite secondo la disciplina recata dal d.lgs. 196/2003.

In ultimo, al fine di agevolare gli operatori nell'attuazione della disciplina vigente nella materia trattata, la cui interpretazione risulta complessa in conseguenza dei molteplici dati di riferimento all'attività dell'Agenzia, contenuti nel testo delle disposizioni, alle presenti indicazioni sono allegati:

- scheda di sintesi legislativa, (**Allegato A**), elaborata a cura della segreteria di direzione, riferita all'analisi del d.lgs. 30 giugno 2003, n. 196 *(Codice in materiali protezione dei dati personali)*, corredata **dagli allegati 1 e 2**, contenenti alcune tavole che riassumono rispettivamente: gli obblighi derivanti all'ARS in ordine alla sua collocazione giuridica e gli obblighi derivanti ai singoli soggetti (titolare, responsabili, incaricati).

- **modulistica semplificata:**
  - clausola di garanzia per trattamento di dati da parte di soggetti esterni all'ARS (**Allegato B);**
  - rinvio a sito Garante per controllo notificazione (**Allegato C**);
  - ipotesi di informativa (**Allegato D**)
  - ipotesi atto di nomina incaricati (**Allegato E**)

IL DIRETTORE
Dott. Francesco Cipriani

INDICE CAPITOLI

11. DIPOSIZIONI FINALI

1. DISPOSIZIONI GENERALI

1.1 Principi generali

Il trattamento dei dati personali deve essere attuato nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
Il trattamento dei dati personali è attuato assicurando un elevato livello di tutela dei diritti e delle libertà, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio.
I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
Le modalità del trattamento devono essere attuate avendo riguardo a trattare i dati personali in modo lecito e secondo correttezza ed in via generale secondo il principio di pertinenza e non di eccedenza; gli stessi devono essere raccolti e registrati ed aggiornati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; infine gli stessi devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
I dati personali trattati in violazione della disciplina rilevante in materia, non possono essere utilizzati.
Il rispetto delle disposizioni contenute nei Codici di deontologia e di buona condotta di cui all'allegato A3 del "Codice", della disciplina contenute nel "Codice di deontologia e di buona condotta per il trattamento dei dati personali per scopi statistici e scientifici" (per ricercatori che operano al di fuori del SISTAN, la cui entrata in vigore è prevista il 1° ottobre prossimo), nonché di tutti i codici emanati per i soggetti pubblici ai sensi dell'art. 106 del d.lgs. 196/2003, in quanto applicabili all'esercizio delle funzioni attribuite all'ARS, costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali effettuati dall'Agenzia. I principi sopra enunciati assumono particolare valore se il trattamento è eseguito per finalità di interesse pubblico che riguardano un terzo o la collettività, ovvero è attuato per scopi statistici o scientifici, con particolare riguardo al trattamento di dati idonei a rilevare lo stato di salute della popolazione previsti dai programmi di ricerca biomedica e sanitaria di cui all'art.12-*bis* del d.lgs. 502/1992 e successive modificazioni
Nei casi predetti, l'intenzione di attenersi alle regole salva - privacy deve essere esplicitata nei progetti di ricerca, nei quali vanno specificate le misure da adottare per la salvaguardia dei dati personali, anche facendo riferimento al documento programmatico sulla sicurezza.
I risultati statistici vanno diffusi soltanto in forma aggregata o secondo modalità che non consentano l'identificazione degli intervistati.
Le informazioni sensibili devono essere trattate in forma anonima; quando non è possibile raggiungere i risultati senza l'identificazione anche temporanea degli interessati, il Responsabile del trattamento deve adottare misure specifiche per mantenere separate le informazioni identificative già al momento della raccolta.
Posto che l'Agenzia, a secondo della tipologia dell'attività svolta è soggetta a disciplina diversa cui conseguono differenti adempimenti da adottare, si rinvia **alle tavole allegate 1 e 2 a corredo dell'All. A** (**scheda sintesi)**.

1.2 Definizioni

Per le seguenti definizioni: *"trattamento", "dato personale", "dati identificativi", "dati sensibili", "titolare", "responsabile", "incaricati", "interessati", "comunicazione", "diffusione", "dato anonimo", "blocco", "banca dati", "Garante", "comunicazione elettronica", "chiamata","reti di comunicazione elettronica" "rete pubblica di comunicazione", "servizi di comunicazione elettronica", "abbonato", "utente", "dati relativi al traffico", "dati relativi all'ubicazione", "servizio a valore aggiunto", "posta elettronica", "misure minime", "strumenti elettronici", autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità; "credenziali di autenticazione", "parola chiave", "profilo di autorizzazione", "sistema di autorizzazione", "scopi statistici", "scopi scientifici",* si fa espresso rinvio al disposto dell'art. 4 del "Codice"e alla legenda fornita a corredo del presente documento.

2. RESPONSABILI DEL TRATTAMENTO E LORO COMPITI

2.1 Individuazione dei Responsabili interni del trattamento

Secondo la disciplina recata dall'art. 82 *duodecies*, comma 2 della l.r. n. 40/2005 e successive modificazioni, i coordinatori degli Osservatori sono i Responsabili del trattamento dei dati personali (comuni, sensibili e giudiziari) effettuati all'interno della rispettiva struttura e per l'ambito di competenza.
Tenuto conto del nuovo assetto dell'Agenzia, non è possibile individuare un Responsabile dei trattamenti afferenti alla Direzione.
Infatti manca all'interno della struttura una figura intermedia fra il direttore (titolare del trattamento) ed i dirigenti (incaricati) quale è invece il coordinatore negli osservatori.
Tuttavia non essendo il Responsabile una figura obbligatoria all'interno dell'architettura del sistema privacy (art. 29, comma 1 del Codice), sarà direttamente il titolare a provvedere alla nomina degli incaricati ed ad avere la responsabilità dei trattamenti afferenti alla direzione.

I Responsabili interni ed esterni e i relativi ambiti di competenza sono specificatamente indicati nelle tabelle che seguono:

RESPONSABILI INTERNI ALL'ARS

STRUTTURE/UFFICI	RESPONSABILE	AMBITI DI COMPETENZA
Direzione: - **Centro documentazione** - **Programmazione e coordinamento strategico** - **Settore Amministrazione**	-	**Nell'ambito dei dati trattati all'interno della struttura di riferimento:** *a)* *dati comuni/sensibili relativi ai componenti degli Organi e alla gestione del rapporto con gli stessi e l'Agenzia;* *b)* *dati comuni/sensibili connessi ad assunzioni, alla stipula di contratti di diritto privato e alla gestione delle risorse umane(compenso, collocamento obbligatorio, assicurazioni integrative, concessione di 1/5 dello stipendio, procedure di conciliazione in materia di rapporto di lavoro, gestione cause di lavoro)* *c)* *dati relativi all'instaurazione e gestione dei rapporti contrattuali con terzi (individuazione del contraente, visura camerale, sottoscrizione contratto ecc;* *d)* *dati relativi alla gestione ai fini contabili di indennità e retribuzioni agli organi e al personale* *e)* *dati comuni/sensibili/giudiziari per la gestione delle cause stragiudiziali* *f)* *dati comuni/sensibili/giudiziari relativi a istruttoria contenzioso giudiziale (affidamento difesa ARS a soggetti esterni, affidamento difesa ARS all'Avvocatura regionale)*

STRUTTURE/UFFICI	RESPONSABILE	AMBITI DI COMPETENZA
Direzione: - **Centro documentazione** - **P.O. Sistemi informatici** - **P.O. Gestione ed analisi flussi sanitari** - **P.O. Tecnologie dell'informazione e comunicazione**	**-**	*a) flussi informativi analitici concernenti i ricoveri ospedalieri,l'erogazione delle prestazioni specialistiche ambulatoriali, di riabilitazione, di assistenza medica convenzionata, di assistenza farmaceutica territoriale e in regime ospedaliero, di trasporto sanitario, le anagrafi egli assistiti, le esenzioni per patologia ed invalidità, i certificati di assistenza al parto, le dimissioni per aborto spontaneo e le interruzioni volontarie di gravidanza;* *b) flussi informativi riguardanti le attività gestionali ed economiche del servizio sanitario e socio-sanitario regionale, nonché i dati di attività e di struttura sanitaria e socio-sanitaria pubblica e privata;* *c) flussi attinenti servizi di elaborazione dati e di verifica di qualità delle aziende sanitarie e delle istituzioni private;* *d) flussi informativi concernenti i dati sulla struttura della popolazione regionale, sull'anagrafe dei residenti, sugli stili di vita, sui fenomeni sociali, sui bisogni reali e sulle risorse;* *e) archivi delle malattie infettive, archivio regionale AIDS;* *f) registro regionale dei difetti congeniti, di mortalità, di dialisi, delle vaccinazioni, dei tumori;* *g) registro INAIL degli infortuni e delle malattie professionali;* *h) altri flussi informativi analitici che abbiano ad oggetto l'attività ospedaliera, le prestazioni sanitarie, socio-sanitarie e sociali erogate sul territorio, le prestazioni di riabilitazione, ulteriori archivi e registri di patologia.*

STRUTTURE/UFFICI	RESPONSABILE	AMBITI DI COMPETENZA
Osservatorio di Epidemiologia	**Coordinatore**	**Nell'ambito dei dati trattati per progetti/programmi di pertinenza degli Osservatori, o per trattamenti effettuati da settori/uffici con funzioni trasversali:** *i) flussi informativi analitici concernenti i ricoveri ospedalieri,l'erogazione delle prestazioni specialistiche ambulatoriali, di riabilitazione, di assistenza medica convenzionata, di assistenza farmaceutica territoriale e in regime ospedaliero, di trasporto sanitario, le anagrafi egli assistiti, le esenzioni per patologia ed invalidità, i certificati di assistenza al parto, le dimissioni per aborto spontaneo e le interruzioni volontarie di gravidanza;* *j) flussi informativi riguardanti le attività gestionali ed economiche del servizio sanitario e socio-sanitario regionale, nonché i dati di attività e di struttura sanitaria e socio-sanitaria pubblica e privata;* *k) flussi attinenti servizi di elaborazione dati e di verifica di qualità delle aziende sanitarie e delle istituzioni private;* *l) flussi informativi concernenti i dati sulla struttura della popolazione regionale, sull'anagrafe dei residenti, sugli stili di vita, sui fenomeni sociali, sui bisogni reali e sulle risorse;* *m) archivi delle malattie infettive, archivio regionale AIDS;* *n) registro regionale dei difetti congeniti, di mortalità, di dialisi, delle vaccinazioni, dei tumori;* *o) registro INAIL degli infortuni e delle malattie professionali;* *p) altri flussi informativi analitici che abbiano ad oggetto l'attività ospedaliera, le prestazioni sanitarie, socio-sanitarie e sociali erogate sul territorio, le prestazioni di riabilitazione, ulteriori archivi e registri di patologia.*
Osservatorio per la Qualità e l'Equità	**Coordinatore**	

2.2. Compiti dei Responsabili

I Responsabili del trattamento dei dati personali compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza; in particolare hanno il dovere di osservare e fare osservare le misure di sicurezza individuate nel successivo paragrafo 6.
I Responsabili del trattamento, ciascuno per le competenze attribuite al paragr. 2.1 devono adempiere agli obblighi indicati nelle tavole[1] che seguono:

SOGGETTI	OBBLIGHI
RESPONSABILE	▪ **Applicare le istruzioni tecniche impartite dal Titolare.** ▪ **Nominare uno o più incaricati in relazione alle esigenze organizzative dell'ente; i compiti attribuiti sono specificati analiticamente per iscritto unitamente alle istruzioni tecniche, che sono impartite avendo a riferimento le prescrizioni contenute nel presente documento.** **I Responsabili, inoltre, collaborano con il Titolare per la privacy e provvedono, avvalendosi del Gruppo Privacy di cui al Cap. 10, a:** ▪ **fornire le informazioni richieste;** ▪ **mettere il Titolare tempestivamente a conoscenza di tutte le questioni rilevanti ai fini del d.lgs. 196/2003;** ▪ **comunicare l'inizio di ogni nuovo trattamento, nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di competenza, ai fini dell'aggiornamento dell'anagrafe dei trattamenti di dati personali dell'Agenzia e dell'eventuale nuova notificazione al Garante;** ▪ **disporre per la tenuta ed aggiornamento del censimento dei trattamenti dei dati personali (CE.TRA) di cui al Cap. 9, anche ai fini dell'adozione del Documento programmatico della sicurezza e per l'eventuale adozione da parte del Titolare di un atto di natura regolamentare con il quale si definisca:** ➢ **i tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni;** ➢ **la disciplina dei rapporti con enti di altre Regioni anche mediante convenzioni (cfr. artt. 20 e 181 "Codice")**[2]. ▪ **proporre al Titolare istanza di autorizzazione al Garante, per il trattamento di dati sensibili qualora l'Agenzia operi come organismo sanitario pubblico (cfr. art. 76 "Codice");** ▪ **predisporre, attraverso il Gruppo Privacy, la notificazione al Garante, sia che l'ARS tratti di dati di tipo sanitario per perseguire finalità collettive, sia per il trattamento per scopi statistici o scientifici (cfr. artt. 37 e 38 "Codice")3;** ▪ **predisporre la comunicazione al Garante per le circostanze di cui all'art. 39 del codice, cioè relativamente al trattamento di dati idonei a rilevare lo stato di salute della popolazione previsti dai programmi di ricerca biomedica e sanitaria di cui all'art. 12- bis d.lgs. 502/1992 e succ. modif. (cfr. art. 39, c.1. lett.b) Codice")4 e relativamente alla comunicazione dei dati personali da parte di un soggetto pubblico all'ARS e viceversa, non previsto da norma di legge o regolamento, effettuata in qualunque forma anche mediante convenzione (cfr. art. 39, comma 1, lett. a) "Codice").**

[2] L'identificazione con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni, è stato adottato con Decreto del Presidente della Giunta regionale 12 febbraio 2013, n. 6/R recante "" *Regolamento di attuazione dell'articolo 1, comma 1, della legge regionale 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)".*"

2.3 Nomina degli incaricati

I Responsabili del trattamento sono tenuti a nominare uno o più incaricati attribuendo loro i profili indicati nelle tavole che seguono.

Amministratore di Sistema: Gestisce il sistema operativo dell'elaboratore (Server o PC) che ospita il Database, eseguendo una serie di operazioni tecniche: dalla configurazione generale al controllo dei diversi momenti di attività.

Amministratore di banca dati (database): Responsabile della progettazione, del controllo e della gestione del database e delle sue prestazioni, dell'affidabilità e delle autorizzazioni all'accesso.

Utente di Database: Per mezzo di un linguaggio interattivo o tramite interfacce opportune, esegue applicazioni predefinite e interrogazioni sul database che non ne comportano la modifica, sia in termini di struttura che di contenuti.

Operatore inserimento dati: *Attraverso opportune interfacce, messe a disposizione dall'Amministratore di banca dati, inserisce i dati nel Database*

[3] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante.

[4] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con forma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice").

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
A) AMMINISTRATORE BANCA DATI CENTRALE **Detto profilo è attribuito per amministrare la banca dati centrale**	**P.O. Gestione ed analisi flussi sanitari** **P.O. Tecnologie dell'informazione e comunicazione**	**DATI COMUNI** **DATI SENSIBILI**	**1) Raccolta:** **a) diretta presso l'interessato;** **b) utilizzo di archivi regionali;** **c) acquisizione archivi da soggetti terzi (pubblici o privati).** **2) Registrazione** **3) Organizzazione** **4) Conservazione** **5) Consultazione** **6) Elaborazione** **7) Modificazione** **8) Selezione** **9) Estrazione** **10) Raffronto** **11) Utilizzo** **12) Interconnessione** **13) Blocco** **14) Comunicazione (autorizzazione Responsabile)** **15) Diffusione (autorizzazione Responsabile)** **16) Gestione della modalità di accesso** **17) Cancellazione** **18) Distruzione**

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
B) AMMINISTRA-TORE DI SISTEMA ***Detto profilo è attribuito per amministrare tutte le banche dati presenti sugli elaboratori elettronici dell'ARS***	**P.O. Sistemi informatici**	**DATI COMUNI** **DATI SENSIBILI**	**1) Raccolta** **a)** diretta presso l'interessato; **b)** utilizzo di archivi regionali; **c)** acquisizione archivi da soggetti terzi (pubblici o privati). **2) Registrazione** **3) Organizzazione** **4) Conservazione** **5) Consultazione** **6) Elaborazione** **7) Modificazione** **8) Selezione** **9) Estrazione** **10) Raffronto** **11) Utilizzo** **12) Interconnessione** **13) Blocco** **14) Comunicazione (autorizzazione Responsabile)** **15) Diffusione (autorizzazione Responsabile)** **16) Gestione della modalità di accesso** **17) Cancellazione** **18) Distruzione**

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
C) AMMINISTRATORE BANCA DATI SPECIFICA ***Detto profilo è attribuito per amministrare una banca dati specifica diversa da quella centrale***	**OSSERVATORI** **P.O. Gestione ed analisi flussi sanitari** **P.O. Tecnologie dell'informazione e comunicazione**	**DATI COMUNI** **DATI SENSIBILI**	**1) Raccolta** **a) diretta presso l'interessato;** **b) utilizzo di archivi regionali;** **c) acquisizione archivi da soggetti terzi (pubblici o privati).** **2) Registrazione** **3) Organizzazione** **4) Conservazione** **5) Consultazione** **6) Elaborazione** **7) Modificazione** **8) Selezione** **9) Estrazione** **10) Raffronto** **11) Utilizzo** **12) Interconnessione con altri dati** **13) Blocco** **14) Comunicazione (autorizzazione Responsabile)** **15) Diffusione (autorizzazione Responsabile)** **16) Gestione delle modalità di accesso** **17) Cancellazione** **18) Distruzione**

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
D) UTENTE BANCA DATI CENTRALE ***Detto profilo è attribuito agli utenti della banca dati centrale***	**OSSERVATORI**	**DATI COMUNI** **DATI SENSIBILI**	**1) Consultazione** **2) Elaborazione** **3) Selezione** **4) Estrazione** **5) Raffronto** **6) Utilizzo** **7) Interconnessione con altri archivi** **8) Comunicazione (autorizzazione Responsabile)** **9) Diffusione (autorizzazione Responsabile)**
E) UTENTE BANCA DATI SPECIFICA ***Detto profilo è attribuito agli utenti di una banca dati specifica diversa da quella centrale***	**OSSERVATORI** **P.O. Gestione ed analisi flussi sanitari** **P.O. Tecnologie dell'informazione e comunicazione**	**DATI COMUNI** **DATI SENSIBILI**	**1) Consultazione** **2) Elaborazione** **3) Selezione** **4) Estrazione** **5) Raffronto** **6) Utilizzo** **7) Interconnessione con altri archivi** **8) Comunicazione (autorizzazione Responsabile)** **9) Diffusione (autorizzazione Responsabile)**

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI	OPERAZIONI
F) AMMINISTRATORE BANCA DATI SPECIFICA	**DIREZIONE:** **P.O. Programmazione e coordinamento strategico**	**DATI SENSIBILI** **DATI GIUDIZIARI**	**1. Raccolta:** **a) diretta presso l'interessato;** **b) acquisizione archivi da altri soggetti esterni (pubblici o privati)** **2. Registrazione** **3. Organizzazione** **4. Conservazione** **5. consultazione** **6. Elaborazione** **7. Modificazione** **8. Selezione** **9. Estrazione** **10. Raffronto** **11. Utilizzo** **12. Blocco** **13. Comunicazione** **14. Diffusione** **15. Cancellazione** **16. Distruzione**
G) OPERATORE INSERIMENTO DATI	**OSSERVATORI** **DIREZIONE**	**DATI SENSIBILI** **DATI COMUNI**	**1) Raccolta** **a) Diretta presso l'interessato;** **b) Utilizzo di archivi regionali;** **c) Acquisizione archivi da soggetti terzi (pubblici o privati).** **2) Registrazione** **3) Consultazione**

3. MODALITA' DEL TRATTAMENTO/CESSAZIONE DEL TRATTAMENTO

3.1 Prescrizioni generali

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto del trattamento devono essere i soli dati essenziali per svolgere attività istituzionali. I dati personali devono essere trattati in modo lecito raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini non incompatibili con tali scopi.
I Responsabili del trattamento sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.
I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito.
I trattamenti di dati effettuati utilizzando le banche dati di diversi Titolari, sono utilizzati previa accordo dei rispettivi Responsabili e ove non rientranti nelle banche dati del territorio regionale, mediante stipula di apposita convenzioni o protocollo d'intesa fra i titolari del trattamento medesimo.
I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

3.2 Prescrizioni specifiche

Al fine di ottemperare alle prescrizioni impartite dal "Codice", i Responsabili del trattamento devono altresì disporre, impartendo opportune prescrizioni agli incaricati, che:

1. l'inizio e la cessazione di ogni trattamento presso ciascuna struttura siano comunicati al referente del Gruppo Privacy di cui al Cap.10, affinché lo stesso provveda:
   a) a trasmettere al componente incaricato del Gruppo medesimo le informazioni utili per la predisposizione degli adempimenti obbligatori per il Titolare, in materia di autorizzazione, notificazione e comunicazione al Garante;
   b) alla tenuta ed aggiornamento del CE.TRA di cui al Cap. 9;
   c) all'aggiornamento (sebbene non più obbligatorio) del Documento programmatico sulla sicurezza di cui al Cap. 6.
2. la nomina degli incaricati o la loro cessazione siano comunicate al referente del Gruppo Privacy, affinché lo stesso provveda a trasmettere le informazioni al componente del Gruppo incaricato della tenuta e aggiornamento dell'anagrafe degli incaricati. Ai fini dell'aggiornamento dell'anagrafe dei Responsabili, il Titolare del trattamento provvede a trasmettere al referente del Gruppo Privacy le informazioni necessarie.

3.2.1 Metodologia di lavoro

Le prescrizioni correlate alla metodologia di lavoro sono finalizzate al perseguimento dei seguenti obiettivi:

1. controllo dell'accesso ai dati;
2. protezione dei dati dalla distruzione;
3. cifratura dei dati;
4. trasferimento sicuro.

Ai fini predetti i Responsabili del trattamento devono attenersi alla seguente metodologia di lavoro, impartendo opportune prescrizioni ai rispettivi incaricati:

1. gli archivi contenenti dati sensibili risiedono fisicamente sulla banca dati centrale (ovvero sui server ad essa dedicati) oppure su apposite cartelle sicure del file server;
2. gli archivi o porzioni di essi contenenti dati sensibili che sono estratti o copiati sui PC e gestiti temporaneamente ai fini del trattamento, al termine dell'elaborazione devono essere distrutti o spostati nelle cartelle suddette;
3. l'accesso a ciascun archivio è regolato dai rispettivi amministratori di banca dati nel rispetto degli incarichi definiti dal Responsabile del trattamento;
4. in ogni archivio i dati individuali (cioè quelli che permettono l'identificazione dei soggetti ad esempio nome, cognome e codice fiscale) dovranno essere separati (in tabelle diverse o files diversi) dai dati sensibili e dovranno poter essere ricongiunti solo dagli amministratori di banca dati;
5. i dati che permettono l'identificazione dei soggetti devono essere crittografati dall'amministratore di banca dati con appositi algoritmi ovvero mediante identificativo universale fornito dalla regione Toscana (IDUNI).

Le procedure indicate ai punti da 1 a 5 sono indispensabili per garantire le prescrizioni minime di sicurezza individuate ad oggi dal Garante.

In considerazione della circostanza che il Codice impone di adottare non solo delle misure minime di sicurezza, ma di adempiere all'obbligo più generale di sicurezza in relazione alle conoscenze tecnologiche e alla specifica natura dei dati trattati, i Responsabili sono incaricati di prevedere graduali modalità per la gestione di tutti gli archivi sulla banca dati centrale, adottando adeguati strumenti di sviluppo.

3.3 Trattamenti di dati affidati all'esterno

In caso di affidamento all'esterno del trattamento di dati, si applicano le seguenti disposizioni:
1. agli Enti, agli organismi, agli altri soggetti esterni all'ARS ed alle strutture accreditate, con esclusivo riferimento alle connesse operazioni di trattamento di dati, è attribuita la qualità di Responsabile ai sensi dell'art. 29 del "Codice";
2. i rapporti intercorrenti fra ARS e soggetti esterni e regolato come segue:
   a) in caso di affidamento di trattamento di dati personali a Enti pubblici o Aziende sanitarie, mediante stipula di apposita convenzione/protocollo d'intesa, attraverso cui sono regolate le intese fra i Responsabili del trattamento, con impegno a sottoscrivere la clausola contemplata al punto 3;
   b) in caso di affidamento a Ditta esterna della messa a punto di sistemi di sicurezza, mediante la stipula di apposito contratto, con impegno a sottoscrivere la clausola di cui al punto 3.
3. Negli accordi con le strutture accreditate e nei contratti di affidamento di attività o di servizi all'esterno dell'Agenzia (outsourcing) deve essere inserita apposita clausola di garanzia (di cui all'All. B), in cui il soggetto accreditato o affidatario s'impegna all'osservanza delle norme di legge sulla protezione dei dati personali e ad osservare quanto disposto dall'ARS in materia di trattamento di dati personali, effettuati in forza del rapporto convenzionale/ contrattuale.

In sede di prima applicazione delle presenti prescrizioni, la strutture competente per la stipula e la conservazione delle convenzioni, protocolli d'intesa e contratti effettua una ricognizione della situazione in essere, al fine di provvedere agli adempimenti di legge, nonché all'inserimento negli atti medesimi delle opportune clausole di garanzia. Copia di tali atti dovrà essere inviata al referente del Gruppo Privacy ai fini della tenuta e aggiornamento del CE.TRA., nonché ai fini della tenuta e dell'aggiornamento dell'elenco delle convenzioni/contratti.

4. NOTIFICAZIONE, COMUNICAZIONE E AUTORIZZAZIONE

Relativamente all'argomento oggetto del presente capitolo (notificazione, comunicazione e autorizzazione), oltre a quanto sottoesposto, si rinvia alle tavole all.1 a corredo dell'allegato A al presente documento.

4.1 Notificazione

La Notificazione è la dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di raccolta e utilizzazione dei dati personali, svolta quale autonomo Titolare del trattamento (art. 37 Codice).
Mentre la normativa previgente stabiliva l'obbligo di notificazione in capo a tutti i soggetti non esplicitamente esentati, il T.U. rovescia l'impostazione e indica solo i pochi casi in cui sussiste l'obbligo in oggetto. L'ARS rientra in tale previsione relativamente al comma 1 lett. b) dell'art. 37 per i trattamenti che riguardano i "*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 dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e monitoraggio della spesa sanitaria*".
Di conseguenza l'ARS soggiace all'obbligo di notificare al Garante il trattamento dei suddetti dati.
La notificazione si effettua con un unico atto ed è eseguita una sola volta indipendentemente dalla durata, dal numero e dal tipo delle operazioni del trattamento, sia che si effettui un solo trattamento, sia che si effettuino più trattamenti con finalità correlate tra loro. Una nuova notificazione è richiesta solo prima della cessazione definitiva del trattamento e prima delle modificazioni agli elementi del trattamento da indicare nella notificazione.
Ogni notificazione inviata al Garante deve essere accompagnata dal pagamento di diritti di segreteria, il cui importo è fissato in euro 150,00.
Per essere valida la notificazione deve essere trasmessa per via telematica utilizzando il modello predisposto dal Garante, disponibile **sul sito web del Garante** www.garanteprivacy.it allegato al presente documento, **sub lett. C),** ed osservando le sue prescrizioni.
Il modello telematico **deve essere sottoscritto con firma digitale**. Il Garante al momento ha stipulato una prima convenzione con le Poste italiane s.p.a., U.N.A.P.P.A., A.L.A.R. per permettere l'esecuzione degli adempimenti "telematici" anche agli enti che non dispongono di firma digitale.
Perché la notificazione sia pienamente efficace è necessario inoltre disporre della conferma di ricevimento della notifica.

Il codice prevede inoltre delle sanzione in ordine al rispetto di detto adempimento:

- Notificazione omessa, incompleta, ritardataria: il Titolare è punito con una sanzione pecuniaria (da 10.000 a 60.000 euro) e con la pena accessoria della pubblicazione dell'ordinanza che applica la sanzione stessa in uno o più giornali, per intero o per estratto;
- Notificazione con notizie non veritiere: la falsa dichiarazione è un reato punito con la reclusione (da 6 mesi a 3 anni, salvo che il fatto configuri reato più grave).

Il Titolare prescrive che i Responsabili del trattamento, avvalendosi del Gruppo Privacy, si attivino per l'adempimento della notificazione.

4.2 Comunicazione

La comunicazione è la dichiarazione con la quale un soggetto pubblico o privato rende note al Garante per la protezione dei dati personali le circostanze di cui all'art. 39, comma 1.
In particolare i Responsabili sono tenuti a predisporre la comunicazione al Garante prima del trattamento nelle seguenti circostanze:

a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione
b) il trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria (ex art 110, comma 1). Come la notificazione anche la comunicazione deve essere trasmessa per via telematica tramite il modello predisposto dal Garante e disponibile sul sito web ufficiale (la scadenza è fissata **per il 30 giugno,** ma al momento non è disponibile il modello sul sito del Garante, quindi non è materialmente possibile adempiere) ed è sottoscritta con firma digitale.

Solo per la comunicazione di dati comuni (ovvero diversi da quelli sensibili), la comunicazione può essere trasmessa anche tramite telefax o lettera raccomandata (artt. 19, co. 2 e 39. comma 1, lett. a) e co. 2, "Codice").

Il codice stabilisce che i trattamenti oggetto di comunicazione **possono iniziare solo dopo 45 gg. dal ricevimento della comunicazione** (salvo diversa determinazione successiva del Garante).

4.3 Autorizzazione

L'autorizzazione è un provvedimento adottato dal Garante con cui il Titolare è autorizzato a trattare determinati dati "sensibili" o giudiziari o a trasferire dati personali all'estero (art. 40). In particolare per quanto riguarda l'ARS questa è sottoposta all'obbligo di chiedere l'autorizzazione SOLO nell'ipotesi in cui l'Agenzia operi come "organismi sanitari pubblici". In questo caso infatti per il trattamento dei dati personali idonei a rivelare lo stato di salute sarebbe possibile solo previa autorizzazione del Garante, autorizzazione rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità (art. 76).

5. DIRITTI DELL'INTERESSATO: CONSENSO / INFORMATIVA

5.1 Consenso

In riferimento al consenso dell'interessato per il trattamento dei dati personali, il "Codice" si basa sul principio del bilanciamento degli interessi: poiché ai soggetti pubblici i trattamenti dei dati personali sono consentiti soltanto per lo svolgimento delle funzioni istituzionali (art. 18, co. 2), e poiché possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute mediante trattamento dati anonimi o comuni (art. 22, co. 3), il Codice dispone che **gli enti pubblici non devono richiedere il consenso.**

Per cui l'ARS, **qualunque sia la tipologia dell'attività svolta, non deve richiedere il consenso dell'interessato.**

Si fa rinvio **alle tavole all. 1, a corredo dell'All. A (scheda sintesi)**.

5.2 Informativa

L'informativa, viceversa è sempre dovuta, a qualsiasi titolo l'ARS esegua il trattamento dei dati.

Anche per questo paragrafo si fa rinvio **alle tavole all. 1, a corredo dell'All. A (scheda sintesi)**.

In merito all'obbligo di informativa si specifica che:

a) ove l'ARS operi come **organismo sanitario pubblico:** l'informativa si attua con modalità semplificata (cfr. art. 77, 79 e 81 del Codice). Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'organismo sanitario pubblico;
b) ove l'ARS operi per **scopi statistici o scientifici**: gli stessi devono essere chiaramente determinati e resi noti all'interessato. L'informativa non è dovuta quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate nei Codici di deontologia e di buona condotta (Art. 105,c. 4 e art. 106 Codice);

c) ove l'ARS operi **come ente pubblico con trattamento di dati comuni (ovvero diversi da quelli sensibili),** l'informativa è resa apponendo apposita clausola sugli atti amministrativi (bandi, avvisi pubblici, ecc), facendo espresso riferimento alle disposizioni del Codice.

Il Responsabile del trattamento dei dati personali deve verificare che gli incaricati forniscano all'interessato oralmente o per iscritto, antecedentemente o al momento della raccolta, l'informativa di cui all'art.13 del Codice relativamente a:

- le finalità per le quali e le modalità con le quali saranno trattati i dati;
- l'obbligatorietà o meno del conferimento dei dati;
- le conseguenze di un eventuale rifiuto a fornire i dati;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- i diritti di cui paragrafo successivo;
- il nome ed il domicilio (e/o la residenza) del Responsabile (o del Titolare).

5.2.1 Diritti dell'interessato

L'interessato ha diritto:

a) di conoscere, mediante accesso gratuito, l'esistenza di trattamenti di dati che possono riguardarlo;

b) di essere informato su:
   1. il nome e il domicilio del Titolare e del Responsabile del trattamento;
   2. le finalità e le modalità del trattamento;
   3. l'eventuale ambito di comunicazione e diffusione;

c) di ottenere a cura del Titolare o del Responsabile, senza ritardo:
   1. la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di 90 giorni;
   2. 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;
   3. l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;
   4. l'attestazione che le operazioni di cui ai punti 2 e 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 riveli impossibile o comporti 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.

Nel caso in cui l'utente intenda presentare ricorso per fatti inerenti al trattamento dei propri dati personali può rivolgere istanza scritta direttamente al Responsabile del trattamento, che procederà agli adempimenti conseguenti. Di ciò dovrà essere informato il Titolare dei trattamenti e il referente del Gruppo Privacy.

L'interessato, nell'esercizio dei diritti sopra riportati può conferire per iscritto, delega o procura a persone fisiche o ad associazioni, mentre se tali diritti sono riferiti a dati personali concernenti persone decedute possono essere esercitati da chiunque vi abbia un interesse giuridicamente rilevante.

6. ADOZIONE MISURE MINIME DI SICUREZZA - DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

6.1 Disposizioni generali

Il Codice dispone che il Titolare nei confronti dei Responsabili e questi ultimi nei confronti degli incaricati, devono dare istruzioni relativamente all'adozione delle misure minime di sicurezza previste. A partire dal febbraio 2012 ARS non ha più l'obbligo del Documento programmatico della sicurezza (entro il 30 giugno – Art. 180, comma 1). Infatti l'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio.
Tuttavia, il Gruppo privacy ha ritenuto mantenere e tenere aggiornato siffatto documento, per non perdere il sistema di protezione che è ancora utile all'Agenzia.

La disciplina della privacy stabilisce che i dati personali oggetto del trattamento devono essere custoditi e controllati in modo da ridurre al minimo i rischi relativi a:

a) distruzione o perdita, anche accidentale, dei dati;
b) accesso non autorizzato;
c) trattamento non consentito o non conforme alle finalità della raccolta.

A tale scopo si deve far riferimento alle conoscenze tecnologiche, alla natura dei dati ed alle specifiche caratteristiche del trattamento.

A fronte di questo obbligo generale di sicurezza, **il Titolare** del trattamento è tenuto a adottare misure minime di sicurezza al fine di assicurare un livello minimo di protezione dei dati personali, e quindi, in questa sede, **impartisce istruzioni ai Responsabili per l'attuazione di tali misure**, come previste dall'art. 34 e 35 del Codice e come specificate dal disciplinare tecnico sulla sicurezza (allegato B del Codice). In particolare, in attuazione della normativa, si stabilisce che le misure che devono essere adottate sono le seguenti:

➔ **per i trattamenti eseguiti con l'ausilio di strumenti elettronici**

- sistema di autenticazione informatica;
- adozione procedure di gestione delle credenziali di autenticazione;
- utilizzazione sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione/manutenzione strumenti informatici;
- protezione degli strumenti elettronici e dei dati rispetto ad accessi non consentiti, trattamenti illeciti e determinati programmi informatici;
- adozione procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- adozione tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rilevare lo stato di salute o la vita sessuale effettuati da organismi sanitari;

➔ **per i trattamenti eseguiti senza l'ausilio di strumenti elettronici**

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione procedure per idonea custodia di atti e documenti affidati agli incaricati o alle P.O.;
- previsione procedure per conservazione di determinati atti in archivi ad accesso selezionato e disciplina modalità di accesso finalizzata all'identificazione degli incaricati.

Si sottolinea che tra le misure di sicurezza previste per il trattamenti eseguiti con l'ausilio degli strumenti informatici, il codice prevede la redazione, e l'aggiornamento annuale, del documento programmatico della sicurezza, nel quale sono elencati tutti i trattamenti dei dati personali, sono analizzati i relativi rischi e le corrispondenti misure di sicurezza da adottare, come è meglio specificato al paragrafo 5.

Di seguito sono descritte le modalità specifiche con cui i Responsabili dovranno adottare le singole misure, così come prescritto dalla normativa:

6.2 Trattamenti con strumenti elettronici

*6.2.1 Sistema di autenticazione informatica**

Gli incaricati devono essere dotati di **credenziali di autenticazione** (per superare la necessità di una procedura relativa ad uno specifico trattamento o ad un insieme di trattamenti) che possono consistere in:

- codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo;
- dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato ad un codice identificativo o ad una parola chiave;
- caratteristica biometria dell'incaricato, eventualmente associato ad un codice identificativo o ad una parola chiave.

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione

Si prescrive inoltre di adottare misure per assicurare la segretezza della componente riservata della credenziale. In particolare:

DISPOSITIVI DI AUTENTICAZIONE	▪ Diligente custodia ▪ Possesso e uso esclusivo dell'incaricato
PAROLA CHIAVE	▪ almeno 8 caratteri. Se lo strumento elettronico non lo permette n massimo caratteri consentito ▪ no riferimenti facilmente riconducibili ad incaricato ▪ modificata da incaricato al primo utilizzo e successivamente almeno ogni 3 mesi (per dati non sensibili ogni 6 m)
CODICE	laddove utilizzato non può essere assegnato ad altri incaricati neppure in tempi diversi
DISATTIVAZIONE CREDENZIALI	▪ credenziali non utilizzate da almeno 6 m (eccetto credenziali autorizzate per soli scopi di gestione tecnica) ▪ perdita della qualità che consente ad incaricato l'accesso ai dati personali
CUSTODIA STRUMENTO ELETTRONICO	Necessità di impartire istruzione ad incaricati per non lasciare incustodito e accessibile il P.C. durante il trattamento
PROLUNGATA ASSENZA O IMPEDIMENTO DELL'INCARICATO	Sono impartite idonee e preventive disposizioni scritte per individuare modalità con cui il Titolare, attraverso i Responsabili, può assicurare la disponibilità di dati o strumenti elettronici in caso di assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema. In questo caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia che devono informare tempestivamente l'incaricato dell'intervento effettuato.

*6.2.2 Sistema di autorizzazione**

Si adotta un sistema di autorizzazione quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso.
Gli ambiti di autorizzazione, individuati per ciascun incaricato o per classi omogenee di incaricati, devono essere configurati prima dell'inizio del trattamento in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
La sussistenza delle condizioni per la conservazione dei profili di autorizzazione deve essere verificata almeno annualmente

** Le disposizioni sul sistema di autenticazione informatica e sul sistema di autorizzazione **non** si applicano ai trattamenti dei dati personali destinati alla diffusione. L'art. 22, comma 8, afferma che i dati idonei a rivelare lo stato di salute non possono essere diffusi.*

6.2.3 Altre misure di sicurezza

- **Individuazione ambito del trattamento consentito ai singoli incaricati e addetti alla gestione/manutenzione degli strumenti informatici**
  Redazione di una lista con aggiornamento periodico (almeno annuale) per individuare l'ambito del trattamento consentito ai singoli incaricati e agli addetti alla gestione o manutenzione degli strumenti elettronici. La lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

- **Rischio di intrusione e programmi ex art. 615 quinquies c.p.**
  Attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale per proteggere i dati dal rischio di intrusione e dall'azione dei programmi ex art. 615-quinquies c.p.

- **Vulnerabilità e difetti strumenti elettronici**
  Aggiornamento periodico almeno semestrale (per i dati non sensibili annuale) dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne i difetti

- **Salvataggio dati**
  Previsione di istruzioni organizzative e tecniche per il salvataggio dei dati con frequenza almeno settimanale

6.2.4 Ulteriori misure in caso di trattamento di dati sensibili

- **Accesso abusivo ex art. 615 ter c.p.**: utilizzo di idonei strumenti elettronici per proteggere dati sensibili e giudiziari contro.

- **Supporti removibili** in cui memorizzare dati sensibili (per evitare accessi non autorizzati e trattamenti non consentiti):
  - i Responsabili devono impartire istruzioni organizzative e tecniche per custodia e uso;
  - se non utilizzati devono essere distrutti o resi inutilizzabili; possono essere riutilizzati da altri incaricati non autorizzati al trattamento dei dati ivi contenuti solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

- **Ipotesi di danneggiamento dei dati o degli strumenti elettronici**: i Responsabili devono adottare misure per garantire il ripristino dell'accesso ai dati in tempi certi compatibili con i diritti degli interessati e comunque non superiore a 7 gg.

- **Dati idonei a rilevare lo stato di salute e la vita sessuale (organismi sanitari o esercenti professioni sanitarie)**

  I Responsabili del trattamento devono attenersi alle seguenti istruzioni:
  - effettuare il trattamento dei dati con le modalità descritte dall'art. 22, comma 6:
    - i dati idonei a rilevare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche dati tenuti con l'ausilio di strumenti elettronici devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi (IDUNI regionale o altro) o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità;
    - tali dati sono conservati separatamente dagli altri dati personali trattati per finalità che non richiedono il loro utilizzo;
    - deve essere consentito il trattamento disgiunto dei dati sensibili dagli altri dati personali che permettono di identificare direttamente gli interessati.

  - I dati relativi all'identità genetica devono essere trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi.
  - Il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti. Il trasferimento in formato elettronico è cifrato.

6.2.5 Altre misure di sicurezza

Il titolare di un trattamento di dati sensibili o di dati giudiziari non è più tenuto a redigere un documento programmatico sulla sicurezza, tuttavia deve attenersi a regole di sicurezza del dato previste dal codice privacy. In particolare:

- elenco trattamenti di dati personali;
- distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- analisi dei rischi che incombono sui dati;
- misure da adottare per garantire integrità e disponibilità dei dati e per proteggere aree e locali, ai fini della custodia e dell'accessibilità dei dati;
- criteri e modalità per ripristino disponibilità dei dati in seguito a distruzione o danneggiamento;
- criteri per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura del Titolare;
- criteri per la cifratura dei dati idonei a rilevare lo stato di salute e la vita sessuale o per la loro separazione dagli altri dati personali dell'interessato;
- formazione degli incaricati al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti rilevanti per il trattamento, relativamente a:
  - rischi che incombono sui dati;
  - misure disponibili per prevenire eventi dannosi;
  - profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
  - responsabilità che ne derivano;

- modalità per aggiornarsi sulle misure minime adottate dal Titolare.

6.3 Trattamenti senza l'ausilio di strumenti elettronici

In caso di trattamento con strumenti diversi da quelli elettronici il Responsabile e l'incaricato devono adottare le seguenti modalità tecniche:

1) Istruzioni scritte agli incaricati relativamente al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
2) Redazione di una lista con aggiornamento periodico (almeno annuale) per individuare l'ambito del trattamento consentito ai singoli incaricati e agli addetti alla gestione o manutenzione degli strumenti elettronici. La lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
3) Gli atti e i documenti contenenti dati sensibili affidati agli incaricati sono controllati e custoditi dagli incaricati stessi fino alla restituzione in modo da impedire l'accesso ai dati da parte di persone prive di autorizzazione. La restituzione avviene al termine delle operazioni affidate.
4) L'accesso agli archivi contenenti dati sensibili è controllato. Le persone ammesse, qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.
5) Se l'archivio è dotato di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

SEGUONO SCHEMI RIASSUNTIVI DELLE MISURE MINIME DI SICUREZZA (con ausilio di supporti informatici e senza tale ausilio)

MISURE MINIME DI SICUREZZA senza ausilio supporti informatici

AGGIORNAMENTO PERIODICO AMBITI TRATTAMENTO CONSENTITO	Redazione di una lista con aggiornamento periodico (almeno annuale) per individuare l'ambito del trattamento consentito ai singoli incaricati e agli addetti alla gestione o manutenzione degli strumenti elettronici. La lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
PROCEDURE PER IDONEA CUSTODIA DI ATTI E DOCUMENTI	Istruzioni scritte agli incaricati relativamente al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali
PROCEDURE PER CONSERVAZIONE DI DETERMINATI ATTI IN ARCHIVI AD ACCESSO SELEZIONATO E DISCIPLINA MODALITÀ DI ACCESSO FINALIZZATA ALL'IDENTIFICAZIONE DEGLI INCARICATI	Gli atti e i documenti contenenti dati sensibili affidati agli incaricati sono controllati e custoditi dagli incaricati stessi fino alla restituzione in modo da impedire l'accesso ai dati da parte di persone prive di autorizzazione. La restituzione avviene al termine delle operazioni affidate.
	L'accesso agli archivi contenenti dati sensibili è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.
	Se l'archivio è dotato di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

MISURE MINIME DI SICUREZZA con ausilio di supporti informatici

SISTEMA DI AUTENTICAZIONE INFORMATICA	Adozione procedure di gestione delle credenziali di autenticazione (codice, dispositivo autenticazione, caratteristica biometria)
SISTEMA DI AUTORIZZAZIONE	individuazione per ciascun incaricato o per classi omogenee di incaricati, prima dell'inizio del trattamento, profili di autorizzazione di ambito diverso
AMBITO CONSENTITO AI SINGOLI INCARICATI E ADDETTI ALLA GESTIONE/MANUTENZIONE PC	Redazione lista incaricati con aggiornamento almeno annuale
PRTOTEZIONE STRUMENTI ELETTRONICI E DATI	- Attivazione di idonei strumenti elettronici da aggiornare semestralmente per proteggere i dati dal rischio di intrusione e dall'azione dei programmi ex art. 615-quinquies c.p. - Aggiornamento semestrale dei programmi per elaboratore volti a prevenire la

(rispetto ad accessi non consentiti, trattamenti illeciti, determinati programmi informatici)	vulnerabilità di strumenti elettronici ed a correggerne i difetti - Previsione di istruzioni organizzative e tecniche per il salvataggio dei dati con frequenza almeno settimanale - Utilizzo di idonei strumenti elettronici per proteggere dati sensibili e giudiziari contro accesso abusivo ex art. 615 ter c.p. - Utilizzo di supporti rimovibili contenti dati sensibili (istruzioni organizzative e tecniche; istruzioni in caso di mancato utilizzo)
PROCEDURE PER CUSTODIA COPIE DI SICUREZZA E RISPRISTINO DISPONIBILITA' DEI DATI E DEI SISTEMI	- Adozione idonee misure per garantire ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi certi compatibili con i diritti degli interessati e comunque non superiori a 7 g
ALTRE MISURE SICUREZZA	- elenco trattamenti di dati personali - distribuzione compiti /responsabilità tra strutture preposte al trattamento. - analisi rischi che incombono sui dati - misure per garantire integrità e disponibilità dei dati e per proteggere aree e locali, ai fini della custodia e dell'accessibilità dei dati - criteri e modalità per ripristino disponibilità dei dati in seguito a distruzione o danneggiamento - criteri per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno - criteri per la cifratura dei dati idonei a rilevare lo stato di salute e la vita sessuale o per la loro separazione dagli altri dati personali dell'interessato - Previsione formazione degli incaricati
TRATTAMENTI DI DATI IDONEI A RILEVARE LO STATO DI SALUTE O LA VITA SESSUALE EFFETTUATI DA ORGANISMI SANITARI	▫ utilizzo tecniche di cifratura o codici identificativi o altre soluzioni per rendere i dati temporaneamente inintelligibili anche a chi è autorizzato e permettere di identificare gli interessati solo in caso di necessità ▫ Possibilità di trattamento disgiunto dei dati sensibili dagli altri dati personali ▫ Dati relativi all'identità genetica trattati solo in locali protetti accessibili ai soli incaricati/soggetti specificatamente autorizzati ad accedervi ▫ Il trasporto dati all'esterno dei suddetti locali in contenitori con serratura o dispositivi equipollenti. Il trasferimento in formato elettronico è cifrato.

7. ACCESSO A FLUSSI DI DATI ATTINENTI ALLA SALUTE AL DI FUORI DELL'AMBITO REGIONALE

L'accesso da parte dell'Agenzia a flussi di dati attinenti alla salute collocati al di fuori dell'ambito regionale sono regolati da apposite convenzioni/protocolli d'intesa, da stipulare con gli Enti interessati.
Il Gruppo Privacy deve procedere alla verifica dei flussi di dati di cui trattasi, proponendo al Titolare, attraverso il Responsabile, l'adozione degli atti necessari. Il medesimo Gruppo ha il compito della tenuta e aggiornamento del registro di detti flussi.
I rapporti fra gli enti ai fini del trattamento dei dati sensibili sono definiti mediante specifiche intese tra i rispettivi Responsabili del trattamento. Dette intese devono trovare conferma nei relativi atti convenzionali o nei protocolli d'intesa.

8. COMUNICAZIONE E DIFFUSIONE DEI DATI

8.1 Comunicazione e Diffusione

La comunicazione consiste nel dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione; la diffusione invece consiste nel dare conoscenza dei dati personali a soggetti indeterminati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
Relativamente ai dati comuni, l'art 19 del codice stabilisce che la comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento

e che, in mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali. Tale comunicazione può essere iniziata decorsi i 45 gg. dalla comunicazione al garante (art. 39 codice).
Relativamente ai dati sensibili l'art. 22 stabilisce che i dati idonei a rivelare lo stato di salute non possono essere diffusi

8.2 Divieti di comunicazione e diffusione dei dati

L'art. 25 dispone il divieto di comunicazione e di diffusione, oltre che in caso di divieto disposto dal Garante o dall'Autorità giudiziaria, in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, ed in riferimento a trattamenti effettuati per finalità diverse da quelle indicate nella notificazione del trattamento.
Inoltre il codice stabilisce che "i dati idonei a rivelare lo stato di salute non possono essere diffusi" (art. 22, comma 8)

8.3 Diritto di accesso ai documenti amministrativi

L'art. 59 del codice sulla privacy in materia di "trattamenti in ambito pubblico" e più precisamente di accesso a documenti amministrativi stabilisce che "i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241 e successive modificazioni "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*.", e dalla altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni eseguibili in esecuzione di una richiesta di accesso".
Tra i limiti dell'esercizio del diritto di accesso la legge n. 241/1990 e ss.mm. prevede appunto il diritto alla riservatezza, e da ciò consegue la necessaria conciliazione delle due esigenze: da una parte il diritto di accesso fondato sul principio di trasparenza, che tuttavia deve essere esercitato con modalità ed accorgimenti tecnici tali da non frustrare l'altro diritto fondamentale, quello della riservatezza. Risulta quindi evidente che, mentre nessun problema si pone per i dati comuni, per quanto riguarda i dati sensibili il bilanciamento tra i valori costituzionali è risolto con la prevalenza del diritto alla riservatezza sul diritto di accesso.

9. CENSIMENTO DEL TRATTAMENTO DEI DATI COMUNI E SENSIBILI (CE.TRA.)

L'ARS istituisce il censimento dei dati personali (CE.TRA.)
Il CE.TRA. contiene la rilevazione dei trattamenti dei dati suddivisi per tipologie e per strutture organizzative ed è tenuto a cura del Gruppo per la Privacy.
Il predetto Gruppo provvede ad aggiornare il CE.TRA., qualora siano comunicati da parte del Titolare o dei Responsabili o degli incaricati del trattamento casi di attivazione di un nuovo trattamento o cessazione di un trattamento in essere.

10. GRUPPO PRIVACY

Considerando l'impatto trasversale del Codice della privacy e il fatto che in ogni struttura complessa (osservatorio e amministrazione centrale) sono svolte operazioni di trattamento, nasce l'opportunità di creare un organismo che abbia una visione di insieme delle attività svolte.
Il d.lgs. 196/2003 infatti richiede una serie di adempimenti, a rilevanza interna ed esterna:

Obblighi a rilevanza interna	Obblighi a rilevanza esterna
Adozione misure di sicurezza.	**Obblighi di informativa all'interessato**
Predisposizione documento programmatico della sicurezza.	**Autorizzazione al Garante.**
Predisposizione atto di natura regolamentare da adottare nel caso in cui l'ARS effettui trattamento di dati oltre quelli identificati dalla legge istitutiva.	**Notificazione al Garante.**
Tenuta e aggiornamento censimento dati (CE.TRA).	**Comunicazione al Garante.**
Tenuta e aggiornamento anagrafe Responsabili e incaricati.	
Tenuta e aggiornamento elenco convenzioni/protocolli/contratti sia per l'affidamento all'esterno del trattamento dei dati sensibili o di sistemi di sicurezza, sia per l'accesso da parte di ARS a flussi di dati presso Enti collocati fuori dell'ambito regionale.	

E' quindi necessaria un'approfondita attività di monitoraggio iniziale (sulle attività svolte nelle varie strutture interessate) ai fini del censimento dei trattamenti effettuati dall'ARS, che richiedono necessariamente il coinvolgimento di più soggetti, con competenze e formazione diversificati. Senza pensare che le misure sicurezza richiedono un aggiornamento, e che l'applicazione della normativa sulla privacy deve essere continuamente monitorata.
Ai fini predetti è istituito un apposito gruppo di lavoro denominato "**Gruppo Privacy**", costituito da diverse professionalità (amministrative, organizzative, tecniche, informatiche, statistiche ecc.).
A ciascun componente sono affidati compiti specifici in relazione alle funzioni attribuite al Gruppo. In seno al gruppo di lavoro è nominato un referente con il compito di programmare, congiuntamente ai membri del Gruppo, le attività necessarie, di trasmettere a ciascun componente le comunicazioni e le informazioni necessarie ai fini degli adempimenti allo stesso spettanti, di controllare le azioni svolte, di relazionare ai Responsabili sulle attività effettuate. Il referente può essere scelto a rotazione tra i componenti del Gruppo medesimo.

Il Gruppo Privacy svolge i seguenti compiti:

1. segnala le novità normative;
2. tiene ed aggiorna:
   a) il censimento dei trattamenti dei dati personali sensibili (CE.TRA) sulla base delle comunicazioni effettuate dai Responsabili del trattamento;
   b) l'elenco degli archivi cartacei e/o magnetici dei dati personali e/o sensibili custoditi dall'Agenzia;
   c) l'anagrafe dei Responsabili e degli incaricati;
   d) l'elenco delle convenzioni/contratti relativi all'affidamento all'esterno del trattamento dei dati;
   e) predisposizione protocollo operativo per trasmissione dati;
3. aggiorna le procedure;
4. assicura la propria collaborazione per la stesura e l'aggiornamento del documento programmatico della sicurezza;
5. collabora con i Responsabili ai processi di formazione e informazione, al fine di sostenere la nascita e la crescita di una cultura del rispetto e della riservatezza a livello di Agenzia.

Al Gruppo sono, altresì, attribuiti compiti di monitoraggio con specifico riguardo alle tipologie di banche dati detenute, sia elettroniche sia cartacee, agli strumenti elettronici utilizzati per il trattamento (elaboratori stand-alone, computer collegati in rete locale, connessione a rete aperta ecc.), ai flussi informativi verso l'esterno e quelli infra-strutture e all'ambito di comunicazione e di diffusione dei dati.

I dati così raccolti saranno utilizzati dal Gruppo Privacy per predisporre la modulistica necessaria (autorizzazione, notificazione, comunicazione, informativa, aggiornamento misure di sicurezza, predisposizione atto di natura regolamentare (ove necessario) e per adempiere agli altri obblighi previsti dalla normativa e dalle presente prescrizioni.

Oltre all'attività di monitoraggio i membri del Gruppo Privacy concorrono con i Responsabili del trattamento, anche alle attività di controllo interno, verificando la corrispondenza e la correttezza delle attività esercitate rispetto a quanto previsto in sede normativa.

Il Gruppo Privacy e costituito dal titolare del trattamenti con atto amministrativo. E' un organismo permanente.

10. DISPOSIZIONI FINALI

Le presenti prescrizioni sono aggiornato a seguito dell'evoluzione del quadro normativo di riferimento, nonché a seguito dell'emanazione da parte del Garante di ulteriori disposizioni in materia.
I Responsabili del trattamento sono tenuti a adeguare le prescrizioni da impartire agli incaricati sulla base dell'aggiornamento del presente documento.

LEGENDA

Trattamento

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

Dati personali

"Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"
I dati personali si distinguono in tre categorie: dati comuni, dati sensibili, dati giudiziari. Quando si fa riferimento ai "dati personali" in genere, si comprende tutte e tre le tipologie di dati.

Dati comuni

"dati personali che permettono l'identificazione diretta dell'interessato".

Dati sensibili

"dati personali idonei a rilevare 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 rilevare lo stato di salute e la vita sessuale".

Dati giudiziari

"dati personali idonei a rilevare provvedimenti di cui all'art. 3, comma 1, lett. da a) a o) e da r) a u) del DPR 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 cpp".

ALLEGATO A

SEGRETERIA DI DIREZIONE

OGGETTO: Decreto legislativo 30 giugno 2003, n. 196 ***(Codice in materia di protezione di dati personali*)**.

Firenze, 10 luglio 2014

Indice: 1. Premessa. 1.1. Analisi generale: I contenuti essenziali e il campo di applicazione.

2.Parte I. Disposizioni generali. 3.Parte II: Disposizioni relative a specifici settori. 3.1.Disposizioni relative a specifici settori. Trattamento di dati in ambito sanitario. 3.2.Trattamento per scopi statistici o scientifici. 4. Indicazioni operative per l'attuazione del provvedimento.

All. A – Schema di sintesi.

1. Premessa

La presente scheda ha come oggetto l'analisi del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione di dati personali) con specifico riferimento all'attività svolta dall'Agenzia regionale di sanità, di seguito indicata come Agenzia; il fine, cioè, che si pone di perseguire è quello di individuare ed esaminare gli aspetti di maggiore connessione rispetto all'attività svolta dall'Agenzia medesima (o all'attività più ampia che nel futuro prossimo l'Agenzia porrà in atto), conformemente al disposto della legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale) Titolo VII, Capo I.

I dati di riferimento normativo sono, dunque, il d.lgs. 196/2003, l'Allegato A), specificatamente l'all. A3 (Trattamento di dati personali per scopi statistici in ambito sanitario e la l.r. n. 40/2005 e ss.mm. citati.

La scheda affronta in una prima parte, in particolare, l'analisi generale del decreto in esame, al fine di fornire un quadro di insieme della normativa specifica; prosegue, poi, su punti specifici con l'obiettivo di fornire suggerimenti ovvero spunti di riflessione per porre in essere gli atti che si ritengono necessari o opportuni per l'attuazione delle disposizioni nazionali in tema di protezione dei dati sensibili.

Il presente elaborato non può essere considerato esaustivo con riguardo a tutti gli aspetti legati alla complessa attività dell'Agenzia ma rappresenta una prima analisi e un punto di partenza al fine di approfondire e valutare successivamente, con l'ausilio eventuale dei responsabili del trattamenti o del personale all'uopo incaricato, gli aspetti di maggior rilievo al fine di garantire la tutela dei dati sensibili nello svolgimento dell'attività da parte dell'Agenzia.

1. ANALISI GENERALE: I CONTENUTI ESSENZIALI E IL CAMPO DI APPLICAZIONE

Il d.lgs. n. 196/2003 e ss.mm. in esame consta dell'unificazione e coordinamento in un unico testo normativo di tutta la copiosa legislazione vigente[5] al momento dell'approvazione del testo unico in materia di protezione di dati personali.

In generale il decreto legislativo in argomento, avendo riguardo agli aspetti di interesse per la natura di ente pubblico dell'Agenzia e per la tipologia dell'attività dalla stessa svolta disciplina:

1. nella **Parte I** – Disposizioni generali – al Titolo III, Capo I (da articolo 11 a 17), disciplina **"Le regole generali per il trattamento dei dati"** dove sono contenute, appunto, le regole per tutti i

[5] Si fa rinvio all'articolo 183 del Codice in materia di abrogazione della legislazione di riferimento abrogata.

trattamenti; al Capo II contiene le **"Regole ulteriori per i soggetti pubblici" (da articolo 18 ad articolo 20).**

Al Titolo IV**,** agli articoli 28, 29 e 30 sono contenute le disposizioni riguardanti i **"Soggetti che effettuano il trattamento"** mentre al Titolo V , dall'articolo 31 all'articolo 36, sono indicate le misure di sicurezza da adottare nel custodire i dati trattati. In questa sede si segnalano le norme in tema di sicurezza da rispettare in tutte l'ipotesi e a seconda delle diverse modalità di raccolta e tenuta dei dati ma non si ritiene opportuno procedere ad un esame analitico in quanto di natura tecnica e non funzionali all'oggetto del presente inquadramento giuridico.

2. Nella **Parte II** – Disposizioni relative a specifici settori- al Titolo V in tema di "Trattamento di dati personali in ambito sanitario" Capo I (articoli 75 e 76) sono contenuti **"I principi generali",** al Capo III (articoli 85 e 86) sono disciplinate le **"Finalità di rilevante interesse pubblico",** al Capo VI (articoli 91, 92, 94) sono contenute disposizioni di varia natura relative, in particolare **a particolari modalità di trattamento di dati sanitari**.

In ultimo, ma non meno importante, si richiama il Capo III "Trattamento per scopi statistici o scientifici" in cui sono contemplate **regole relative al trattamento di dati sensibili con riguardo al trattamento per scopi scientifici,** finalità che caratterizza in modo precipuo l'attività dell'Agenzia.

E' evidente già dal panorama normativo ora delineato che molteplici sono i dati di riferimento contenuti nel testo unico in esame ed, in conseguenza, complessa è l'attività di coordinamento richiesta all'interprete al fine di delineare in maniera corretta e chiara il quadro normativo di riferimento che si riferisce all'attività dell'Agenzia.

2. ESAME DELL'ARTICOLATO

Parte I. Disposizioni generali.

Ai fini del presente elaborato, è opportuno soffermarsi solo sugli aspetti salienti della parte generale, e rinviare ad un esame più dettagliato nella parte relativa al trattamento dei dati relativi ai settori specifici.

In particolare l'articolo 2, comma 1, del testo in esame individua, come finalità della intera disciplina, la garanzia *"che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali"*. Al comma 2 sono enucleati i principi generali ispiratori che devono caratterizzare le modalità del l'adempimento degli obblighi da parte dei titolari del trattamento e segnatamente il principio di *"di semplificazione, armonizzazione ed efficacia"*.

Ai sensi dell'articolo 4, si intende per trattamento *"qualunque operazione o complesso di operazioni effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati"*. Ancora, al fine di fornire un'indicazione tecnico-giuridica precisa in ordine all'uso dei termini più ricorrenti, la norma definisce sono dati sensibili, per quel che rileva ai fini del presente lavoro, "i *dati personali idonei a rivelare lo stato di salute e la vita sessuale"*

dell'interessato (cioè di colui al quale si riferiscono i dati); individua come "titolare" del trattamento *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"*. In ultimo la norma in esame indica come responsabile del trattamento *" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali"* ed in ultimo, ancora, indica come incaricati al trattamento *"le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile"*.

Per quanto concerne le regole generali per tutti i trattamenti dei dati, l'articolo 11 enuclea una serie di punti fondamentali in ordine alle modalità del trattamento, modalità che devono ispirarsi ai principi di liceità e correttezza, per scopi determinati, espliciti e legittimi; i dati trattati devono essere esatti ed aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti, devono essere conservati *"in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati"*.

Agli articoli 18, 19 e 20 del d.lgs. in esame sono contenuti alcuni principi fondamentali riguardanti le regole "*ulteriori"* (rispetto a quelle cui, se pur in breve, si è fatto cenno sopra) valide per i soggetti pubblici (esclusi gli enti pubblici economici); analizzando la disciplina in essi contenuta si può affermare che l'articolo 18 disciplina i principi applicabili in generale a tutti i trattamenti, prevedendo, in particolare, al comma 2, che *"qualunque trattamento di dati personali (…) è consentito soltanto per lo svolgimento delle funzioni istituzionali"* e *"salvo quanto previsto (..) per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato"*.

E' degno di nota, già dall'analisi che precede come il trattamento dei dati sanitari rappresenti un'ipotesi particolare; è importante segnalare questo aspetto per quanto potrà evincersi nell'analisi delle disposizioni specifiche contenuta nella **Parte II.**

Proseguendo, gli articolo 19, 20 e 21 si occupano, rispettivamente, l'articolo 19 dei principi applicabili al trattamento da parte, sempre, degli enti pubblici, di dati diversi da quelli sensibili e giudiziari mentre gli articoli 20 e 21 disciplinano il trattamento dei dati sensibili.

Ritenendo rilevante soffermarsi in questa sede sulle disposizioni in tema di trattamento di dati sensibili, i citati articoli 20 e 21 enucleano i seguenti principi:

- Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito *"solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite"*.
- Nell'ipotesi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico ma non i tipi di dati e di operazioni eseguibili "*il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare (..)"*. L'identificazione dei tipi di dati e di operazioni è aggiornata e integrata periodicamente.
- I dati sensibili *"contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la*

natura dei dati trattati, li rendono temporaneamente intelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".

- I dati idonei a rivelare lo stato di salute non possono essere diffusi.

****

Le regole generali ora descritte richiedono un breve disamina che, poi, sarà ripresa più diffusamente nel paragrafo relativo agli adempimenti necessari ed opportuni riguardanti più specificamente l'attività dell'Agenzia. E' in questo momento importante evidenziare come ai sensi della disposizione citata, è necessario per l'ente pubblico adottare un atto di natura regolamentare nell'ipotesi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico ma non i tipi di dati e di operazioni eseguibili di guisa da ritenersi necessario un atto di tipo integrativo (di natura regolamentare, appunto) della legge autorizzativa del trattamento che specifichi i tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti a cura dei soggetti che effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi.

Parte II: disposizioni relative a specifici settori

2.1. Trattamento di dati in ambito sanitario.

Il d.lgs. in esame dedica un'ampia trattazione con riguardo ai dati in ambito sanitario. Dalle disposizioni in esso contenute, tuttavia, emerge una prima considerazione di ordine generale che attiene al dato che le disposizioni riguardano prevalentemente i soggetti sanitari (medici) e le strutture pubbliche o private che erogano direttamente prestazioni di natura sanitaria.

Alla luce di tale considerazione generale, dunque, è prioritario verificare se l'Agenzia possa collocarsi dal punto di vista giuridico e normativo nell'ambito "degli organismi sanitari pubblici" che, ai sensi degli articoli 76 e ss. del d.lgs. in esame, sono destinatari della disciplina sul trattamento dei dati personali in ambito sanitario. Tale verifica si ritiene, oltretutto, importante perché l'applicazione delle disposizioni in esame comporta, come si vedrà, la necessità per l'Agenzia di acquisire la richiesta di autorizzazione al trattamento da inoltrare al Garante ai sensi dell'articolo76 del d.lgs. in esame.

Si è tenuto a precisare che l'analisi che segue attiene ad aspetti squisitamente giuridici e normativi in quanto la collocazione dell'Agenzia tra gli organismi sanitari pubblici ai quali fa riferimento il decreto probabilmente non può prescindere dalla conoscenza diretta del tipo di attività che svolge (o verrà a svolgere o potrebbe svolgere l'Agenzia) e delle modalità di trattamento dei dati, conoscenza che può essere oggetto di approfondimento in un momento successivo alla predisposizione della presente scheda.

****

Certamente l'Agenzia non è struttura che direttamente eroga prestazioni sanitarie. Tuttavia la sua qualificazione di organismo sanitario pubblico si ritiene non possa escludersi a priori ma al contrario si ritiene possa affermarsi sulla scorta delle considerazioni che seguono.

Ai sensi dell'articolo 76 del d.lgs. in esame, infatti, sono organismi sanitari pubblici*, quelli che "anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute (….) "* per perseguire la finalità di tutela della salute di un terzo o della collettività.

Ai sensi dell'articolo 85 (rubricato "Compiti del Servizio sanitario nazionale"), poi, si precisa che si considerano finalità di rilevante interesse pubblico le finalità che rientrano *"nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative",* tra l'altro, all'attività di *"programmazione, gestione, controllo e valutazione dell'assistenza sanitaria".*

Si ritiene che l'analisi che precede fornisca elementi di per sé sufficienti a collocare l'Agenzia nell'ambito degli organismi sanitari pubblici ancorché non eroghi direttamente prestazioni sanitarie. Tuttavia a maggiore conferma di tale risultato si deve, poi, ricordare che l'enucleazione delle finalità che rientrano nei compiti del Servizio sanitario nazionale, potrebbe non risultare esaustiva perché oggetto di possibile integrazione con le ulteriori finalità di rilevante interesse pubblico individuate dalle regioni come accade, in particolare, nel caso in esame, dalla normativa della Regione Toscana

Il passaggio ora delineato è strettamente connesso con la trattazione di ben più ampio respiro legata alla modifica del Titolo V della Costituzione ed, in particolare, alle rilevanti modifiche in ordine alla competenza legislativa delle regioni, anche in materia sanitaria che pur restando una competenza concorrente con la competenza statale, per il mutato quadro complessivo a livello costituzionale, può dirsi aver acquistato ben più ampia portata.

Non è questa la sede per simile approfondimento, tuttavia sia sufficiente notare che la Regione Toscana ha senza dubbio attribuito all'Agenzia un ruolo di rilevante interesse pubblico nell'ambito del Servizio sanitario regionale nel momento in cui, all'articolo 82 della l.r. n. 40/2005 ad essa attribuisce importanti funzioni di supporto e consulenza al Consiglio, alla Giunta ed ad altri soggetti pubblici e privati in materia, tra l'altro, di programmazione regionale, valutazione della sanità regionale, valutazione della programmazione, analisi dei modelli organizzativi e gestionali.

Alla luce delle considerazioni svolte, ne discende come conseguenza l'applicazione del disposto dell'articolo 76, comma 1, lett. b), già in precedenza citato, secondo il quale *"Gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute (..) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di (..) "* tutela della salute *" riguarda un terzo o la collettività".*

Dall'analisi fin qui svolta, in particolare dal combinato disposto degli articoli 20 e 76 il quadro giuridico di riferimento appare così delineato: l'Agenzia, in quanto ente pubblico autorizzato al trattamento dei dati sensibili da espressa previsione legislativa nella quale, in modo piuttosto completo, sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite, qualora tratti dati di tipo sanitario per perseguire finalità collettive, necessita di previa autorizzazione del garante:

Tuttavia, per diretta conoscenza dell'attività svolta e, quindi, in considerazione della tipologia dei dati da trattare e delle operazioni di trattamento da eseguire, non si è riscontra una previsione legislativa completa, percui si è resa necessaria l'adozione da parte della Regione Toscana di un atto che, sulla base delle disposizioni contenute nella l.r. n. 40/2005, precisi i dati e le operazione eseguibili, a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi (..), è stato adottato, in conformità al parere[6] espresso dal Garante ai sensi dell'articolo 154, comma 1, lett. g), un atto di natura regolamentare.

[6] Il parere previsto appare atto diverso dall'autorizzazione al trattamento di dati sanitari richiesto all'articolo 76, comma 1, lett. b), in ogni caso necessaria qualora, si ripete, si tratti di dati sensibili idonei a rivelare lo stato di salute.

Il nuovo regolamento è entrato in vigore a febbraio 2013, con la pubblicazione sul BURT n. 7 del 15 febbraio 2013, Parte Prima, del DECRETO DEL PRESIDENTE DELLA GIUNTA REGIONALE 12 febbraio 2013, n. 6/R, recante "*Regolamento di attuazione dell´articolo 1, comma 1, della legge regionale 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)"."* .

All'interno dello stesso è prevista un'apposita scheda (la n. 12) all'Allegato A) che appunto integra rispetto alla legge regionale n. 40/2005, i dati che l'Agenzia può trattare.

A seguito di vari incontri con i competenti uffici regionali, la portata del regolamento suddetto è stata ampliata. I dati, infatti, trattabili da ARS non sono solo quelli elencati nei diciotto flussi censiti, ma anche quelli che sono ad essi variamente collegati.

2.2. Trattamento per scopi statistici o scientifici

La tipologia dell'attività svolta dall'Agenzia rientra a pieno titolo, o forse sarebbe più opportuno dire *naturaliter,* cioè per sua vocazione naturale*,* nell'ambito della disciplina del trattamento per scopi scientifici contenuta al Capo III agli articoli 104 e seguenti del decreto.

Le disposizioni contenute in questo Capo in generale sono tese a garantire il corretto utilizzo di dati raccolti inizialmente per altri scopi, si pensi allo scopo sanitario, e dunque tese a garantire il corretto utilizzo ed il rispetto, nel caso di specie, della finalità scientifica.

Da qui la previsione del rispetto di codici di deontologia e di buona condotta (articolo 106) di cui il Garante è promotore, nei quali è prevista tutta una dettagliata serie di disposizioni atte a garantire la correttezza del trattamento dei dati.

Ai fini della presente esposizione, rilevano gli articoli 109 e 110 che, espressamente, si occupano di dati sanitari. In particolare l'articolo 110 in tema di ricerca medica, biomedica ed epidemiologica prevede che *"Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12 bis del decreto legislativo 30 dicembre 1992, n. 502 e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39".*

2.3. Trattamento dati comuni (o diversi da quelli sensibili).

Gli articoli 11, 12 e 18 del "Codice" disciplinano le modalità del trattamento dei dati personali effettuati da soggetti pubblici. Il trattamento da parte di un soggetto pubblico riguardanti dati comuni o diversi da quelli sensibili o giudiziari è consentito, per lo svolgimento delle funzioni istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente (Art. 19, comma 1, "Codice"). Il trattamento deve comunque avvenire nel rispetto delle disposizioni del "Codice" e dei Codici di deontologia e buona condotta.

3. INDICAZIONI OPERATIVE PER L'ATTUAZIONE DELLA NUOVA DISCIPLINA

Si procede ad un'elencazione schematica dei punti trattati. Per esigenze di chiarezza si utilizza il metodo della elencazione con la precisazione, però, necessaria, che trattasi di punti tra loro collegati e difficilmente separabili.

3.1 Individuazione dei responsabili .

Il dato normativo fin qui esaminato induce a ritenere che il primo passaggio che l'Agenzia, quale titolare del trattamento dei dati, è opportuno compia sia posto nella individuazione dei responsabili del trattamento. La legge regionale n. 40/2005 e ss.mm., in realtà, all'articolo 82 novies decies, comma 2, individua già i responsabili del trattamento in relazione alle strutture dalla stessa legge individuate, nelle figure, appunto, dei coordinatori degli osservatori. Comunque si ritiene opportuno procedere nei sensi predetti, pur in presenza del disposto normativo, dovendo il titolare procedere ad impartire ai responsabili precise indicazioni tecniche, ivi compreso il profilo di sicurezza, oltrechè individuare i rispettivi ambiti di competenza. Si reputa, altresì, secondo il disposto dell'art. 29 che, ove il titolare ne ravvisi la necessità, in relazione ad esigenze organizzative legate alla struttura operativa, sia possibile individuare ulteriori figure di responsabili del trattamento, in coerenza agli indirizzi organizzativi impartiti, con atti amministrativi, dai competenti organi, secondo la disciplina vigente in materia. I responsabili del trattamento sono tenuti a rispettare le indicazioni tecniche impartite dal titolare del trattamento, ivi compreso il profilo di sicurezza.

3.2 Nomina degli incaricati.

I responsabili del trattamento devono procedere alla nomina per iscritto degli incaricati al trattamento. Quest'ultimi sono soggetti al rispetto delle indicazioni tecniche impartire dai responsabili, ivi compreso il profilo di sicurezza. La nomina degli incaricati avviene con nota avente data certa e protocollata, secondo il modello predisposto ed allegato sub lettera E)

3.3 Trattamento dati sensibili. Autorizzazione del Garante.

Il decreto considera, in generale, **l'ente pubblico quale soggetto autorizzato** al trattamento dei dati sensibili in forza di una legge specifica (si veda il punto 3.9 successivo) e, solo nel caso di trattamento di **dati sanitari effettuato per la tutela della salute e incolumità che riguardi un terzo** (cioè non l'interessato) **ovvero la collettività,** richiede **l'autorizzazione del Garante** ai sensi dell'articolo 76, comma 1, lett. b).

3.4 Trattamento dati sensibili. Obblighi di notificazione al Garante.

La notificazione è presentata al Garante prima dell'inizio del trattamento (art. 38, comma 1) ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare e può riguardare uno o più trattamenti con finalità correlate. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento dei dati all'estero. La stessa è validamente effettuata solo se è trasmessa in via telematica utilizzando il modello predisposto dal Garante ed osservando le prescrizioni da questo impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma di ricevimento della notificazione. Le notificazioni sono inserite in un registro pubblico che sarà consultabile gratuitamente da tutti *on-line.*

Ogni notificazione inviata al Garante deve essere accompagnata dal pagamento di diritti di segreteria, il cui importo è fissato in euro 150,00. Per perfezionare la notificazione è necessario sottoscriverla con firma digitale (art. 10, comma 3 d.p.r. 445/2000). A tal fine il titolare del trattamento deve utilizzare un dispositivo di

firma digitale disponibile presso uno dei certificatori accreditati ai sensi dell'art. 2, comma 1, lett. c) d.lgs. n. 10/2002. L'elenco dei certificatori è rinvenibile sul sito www.cnipa.gov.it.

Il Garante al momento ha stipulato una prima convenzione con le Poste Italiane Spa per permettere l'inoltro della notificazione tramite gli uffici PT *business.*

Il titolare che abbia iniziato il trattamento anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che lo abbia notificato in passato, deve procedere, se vi è tenuto (è previsto obbligo di notifica nel caso di trattamento di dati sensibili), entro il 30 aprile 2004 (art. 181, comma 1, lett. c).

Sul sito Internet del Garante https://web.garanteprivacy.it/rgt/. è disponibile la normativa, una guida per la compilazione della notificazione ed il relativo modello.

Al riguardo si sottolinea che, per quanto riguarda le scadenze il Codice stabilisce che per le attività di trattamento che non esistevano prima del 1° gennaio 2004 la notificazione va effettuata prima che inizi il trattamento stesso; mentre per le attività che erano già in essere prima del 1° gennaio 2004, la notificazione doveva essere effettuata entro il 30 aprile 2004 (art. 181, comma 1, lett. c). Il Codice prevede inoltre delle sanzione in ordine al rispetto di detto adempimento:

- **Notificazione omessa, incompleta, ritardataria: il Titolare viene punito con una sanzione pecuniaria (da 10.000 a 60.000 euro) e con la pena accessoria della pubblicazione dell'ordinanza che applica la sanzione stessa in uno o più giornali, per intero o per estratto;**
- **Notificazione con notizie non veritiere: la falsa dichiarazione è un reato punito con la reclusione (da 6 mesi a 3 anni, salvo che il fatto configuri reato più grave).**

3.5 Trattamento dati sensibili. Obblighi di comunicazione al Garante.

L'art. 39, comma 1, lett. b), prevede l'obbligo per il titolare del trattamento di comunicare al Garante, il trattamento di dati idonei a rilevare lo stato di salute, previsto dal programma di ricerca biomedica o sanitaria di cui all'art. 12-*bis* del d.lgs. 502/1992 e successive modificazioni. **Per ARS la comunicazione è stata effettuata entro il 30 giugno 2004 (art. 181, comma 1, lett. d).**

3.6 Trattamento dati sensibili. Consenso dell'interessato.

Il "Codice" sviluppa il principio del bilanciamento degli interessi di tutela con uno snellimento degli adempimenti a carico degli Enti, L'area del consenso è sostanzialmente confermata rispetto all'ordinamento previgente, con l'individuazione di alcune ipotesi di esonero.

Nell'ambito della tipologia dell'attività svolta dall'Agenzia, avente la finalità di tutela della salute riguardante un terzo o la collettività, ai sensi dell'articolo 76, comma 1, lett. b) del Codice il trattamento dei dati sensibili non richiede il consenso dell'interessato. Analogamente per il trattamento di dati sensibili finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico qualora, come nel caso dell'Agenzia, appunto, la ricerca sia prevista da una disposizione di legge che prevede specificamente il trattamento.

3.7 Trattamento dati sensibili. Informativa all'interessato.

Rimane fermo l'adempimento dell'informativa all'interessato preventiva al trattamento di tutti dati.

3.8 Trattamento dati comuni (o diversi da quelli sensibili).

In detta fattispecie l'Agenzia **non è soggetta ad autorizzazione del Garante**, **né a richiedere il consenso dell'interessato** (art. 18 e 19). **E', altresì, escluso l'obbligo di notificazione al Garante**

E' viceversa soggetta:

- **all'obbligo di comunicazione preventiva al Garante**, **nel caso di comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico** non previsto da norma di legge o regolamento, effettuata in qualsiasi firma anche mediante convenzione. La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con forma digitale e conferma del ricevimento della notificazione (art. 39, comma 1, lett. a) e comma 2, "Codice"). La comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico è ammessa quando è prevista da norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento delle funzioni istituzionali (Art. 19, comma 2). La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione sono ammesse solo se previste da legge o regolamento (Art. 19, comma 3).

  La comunicazione è stata effettuata per ARS entro 30 giugno 2004.

- **all'obbligo d'informare l'interessato, salvo che i dati siano trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria (art. 13 "Codice");**
- **a adottare la busta chiusa per i casi di notifica a persona diversa dal destinatario degli atti amministrativi**. Trattasi d'innovazione introdotta dal Codice, in accoglimento delle indicazioni del Garante, in materia di notificazione degli atti amministrativi e giudiziari.

3.9 Atto di natura regolamentare

Punto che richiede, invece, soluzioni più articolate attiene alle regole di natura tecnica legate al trattamento dei dati. In questa sede si fa riferimento alle disposizioni contenute all'articolo 20 il quale, come si ricorda, nel caso di trattamento di dati sensibili da parte di enti pubblici, prevede la necessità di un atto di natura regolamentare a seconda che i tipi di dati che possono essere trattati e le operazioni eseguibili nonché le finalità di rilevante interesse pubblico sottese al trattamento siano o meno specificate in una legge. Nel caso dell'Agenzia la legge regionale n. 40/2005 e ss.mm. contiene tutta una serie di indicazioni. In conseguenza, si è ritenuto di poter ravvisare la necessità di adottare un atto ulteriore, al fine di garanzia della correttezza e sicurezza del trattamento., tutto questo per effetto dello sviluppo dell'attività dell'Ente, e vista l'esigenza di ricerca che è andata oltre i dati indicati dalla legge istitutiva.

Il regolamento regionale infatti prevede l'integrazione e specificazione dei tipi di dati e delle relative operazioni eseguibili che, per effetto dello sviluppo delle attività dell'Ente, possono essere trattati in aggiunta a quelli già identificati dalla legge istitutiva.

3.10 <u>Altre misure di sicurezza.</u>

Con riguardo alle modalità del trattamento e, più in particolare, alle misure di sicurezza da adottare, occorreva, nel caso del trattamento di dati sensibili con l'ausilio di strumentazione elettronica, adottare, ai sensi dell'articolo 35 del Codice, un documento programmatico della sicurezza conformemente al contenuto ed alle indicazioni a tal riguardo indicate negli articoli da 33 a 36 e nell'allegato B del Codice. Tale adempimento non è più obbligatorio per ARS, ma il Gruppo privacy ha ritenuto opportuno mantenere il sistema di protezione e sicurezza in esso contenuti.

Il C.d.A. ha quindi dovuto adottare con atto deliberativo, che per chiarezza definiamo atto amministrativo, il "Documento programmatico sulla sicurezza", nel quale sono state definite, anche in base allo schema predisposto dal Garante e consultabile sul sito dello stesso, le misure di sicurezza e tutte le disposizioni che regolamentano, dal punto di vista tecnico, il trattamento dei dati.

3.11 Comunicazione di dati sensibili tra enti pubblici non previsti dalla legge. Chiariti gli aspetti finora elencati resta da affrontare, in questa fase in modo schematico, l'aspetto riguardante il trattamento di dati sensibili acquisiti da altri enti diversi da quelli contemplati dalla legge regionale 22/2000, ed in particolare enti collocati fuori dalla Regione Toscana. Si potrebbe ipotizzare la necessità di accordi convenzionali, o protocolli di intesa con gli enti interessati, per la comunicazione dei dati di interesse magari individuati previamente da parte dell'Agenzia in sede di programmazione pluriennale. In detti accordi o protocolli gli Enti interessati dovranno reciprocamente dare atto che il trattamento avverrà nel rispetto della disciplina recata dal "Codice", delle prescrizioni emanate dai rispettivi enti, nonché delle disposizioni contenuti nei codici di deontologia con diretto riflesso al tipo di trattamento effettuato.

La scheda è corredata da due tavole All. 1 e 2 che riassumono rispettivamente gli obblighi derivanti all'ARS in ordine alla sua collocazione giuridica e gli obblighi derivanti per i singoli soggetti (titolari, responsabili e incaricati), in attuazione del disposto di cui al decreto legislativo in esame.

ALLEGATO 1

ARS TOSCANA
agenzia regionale di sanità

L'ARS NELLA DISCIPLINA DEL
DECRETO LEGISLATIVO 30 giugno 2003, n. 196
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

TIPOLOGIA	AUTORIZ-ZAZIONE GARANTE (Art. 20)	NOTIFICA-ZIONE AL GARANTE (Artt. 37, co. 1, lett. b) e 38)[7]	COMUNICAZIONE AL GARANTE (Artt. 39 e 110)[8]	CONSENSO INTERES-SATO (Artt. 18, co. 4 e 20)	INFORMATIVA INTERESSATO (Artt. 13 e 22)	REGOLA-MENTO DATI SENSIBILI (Art. 20)[9]	DOCUMENTO PROGRAM-MATICO SICUREZZA[10] (Art. 34, co. 1. lett. G) e All. B)
ENTE PUBBLICO Trattamento dati sensibili	**NO**	**SI**	**SI** ***ove si tratti di trattamento di dati idonei a rilevare lo stato di salute previsto da un programma di ricerca biomedica o sanitaria di cui all'art. 12 bis del d.lgs. 502/'92 e successive modificazioni.***	**NO**	**SI, f*acendo espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili.***	**SI** ***ove si tratti dati diversi da quelli identificati nella legge istitutiva.***	**SI**

[7] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante. Il titolare che abbia iniziato il trattamento anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che lo abbia notificato in passato, deve procedere, se vi è tenuto, entro il 30 aprile 2004 (art. 181, comma 1, lett. c).

[8] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice"). La comunicazione è effettuata entro il 30 giugno 2004 (art. 181, comma 1, lett. d).

[9] L'identificazione è avvenuta con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni. ARS non ha potestà regolamentare, quindi è inserita nell'ambito del regolamento privacy della Regione Toscana. Nello specifico con la pubblicazione sul BURT n. 7 del 15 febbraio 2013, Parte Prima, del DECRETO DEL PRESIDENTE DELLA GIUNTA REGIONALE 12 febbraio 2013, n. 6/R è entrato in vigore il " Regolamento di attuazione dell´articolo 1, comma 1, della legge regionale 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)". L'emanazione del presente Regolamento ha comportato la contestuale abrogazione del precedente regolamento di pari oggetto (DPRG 18/R/2006). La disciplina per ARS è inserita nella scheda n. 12 Allegato A) (cfr. artt. 20 e 181 "Codice").

[10] L'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio

TIPOLOGIA	AUTORIZ-ZAZIONE GARANTE (Art. 76, co. 1, lett. b)	NOTIFICA-ZIONE AL GARANTE (Artt. 37, co. 1, lett. b) e 38)[11]	COMUNICA-ZIONE AL GARANTE (Art. 39, co. 1, lett. b)[12]	CONSENSO INTERES-SATO (Art. 76, co. 1, lett. b)	INFORMATIVA INTERESSATO (Artt. 77 e 79)	REGOLA-MENTO DATI[13] (Art. 20)	DOCUMENTO PROGRAMMA-TICO SICUREZZA[14] (Art. 34, co. 1, lett. g) e All. B)
ORGANISMO SANITARIO PUBBLICO L'ARS, ancorché non eroghi prestazioni sanitarie, rientra tra gli organismi sanitari pubblici qualora tratti dati di tipo sanitario per perseguire finalità d'interesse pubblico che riguardi un terzo o la collettività.	**SI,** ***rilasciata dal Garante sentito il Consiglio superiore di Sanità.***	**SI**	**SI** ***ove si tratti di trattamento di dati idonei a rilevare lo stato di salute previsto da un programma di ricerca biomedica o sanitaria di cui all'art. 12 bis del d.lgs. 502/'92 e successive modificazio-ni.***	**NO**	**SI** ***con moda-lità semplifi-cata.***	**SI,** ***ove si tratti dati diversi da quelli identificati nella legge istitutiva.***	**NO**

[11] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante. Il titolare che abbia iniziato il trattamento anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che lo abbia notificato in passato, deve procedere, se vi è tenuto, entro il 30 aprile 2004 (art. 181, comma 1, lett. c).

[12] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice").

L'identificazione è avvenuta con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni. ARS non ha potestà regolamentare, quindi è inserita nell'ambito del regolamento privacy della Regione Toscana. Nello specifico con la pubblicazione sul BURT n. 7 del 15 febbraio 2013, Parte Prima, del DECRETO DEL PRESIDENTE DELLA GIUNTA REGIONALE 12 febbraio 2013, n. 6/R è entrato in vigore il " Regolamento di attuazione dell´articolo 1, comma 1, della legge regionale 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)". L'emanazione del presente Regolamento ha comportato la contestuale abrogazione del precedente regolamento di pari oggetto (DPRG 18/R/2006). La disciplina per ARS è inserita nella scheda n. 12 Allegato A) (cfr. artt. 20 e 181 "Codice").

[14] L'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio.

TIPOLOGIA	AUTORIZ-ZAZIONE GARANTE (Art. 20)	NOTIFICA-ZIONE AL GARANTE (Artt. 37, co. 1, lett. b e 38[15])	COMUNICA-ZIONE AL GARANTE (Art. 39, co. 1, lett. b)[16]	CONSENSO INTERES-SATO (Art. 110)	INFORMATIVA INTERESSATO (Artt. 13,105, 106, co.1, lett. b)	REGOLA-MENTO DATI[17] (Art. 20)	DOCUMENTO PROGRAMMA-TICO SICUREZZA[18] (Art. 34, co. 1, lett. g) e All. B)
TRATTAMENTO DATI SENSIBILI PER SCOPI STATISTICI O SCIENTIFICI[19] **Ricerca medica, biomedica ed epidemiologi-ca**	**NO**	**SI**	**SI** ***trattamento di dati idonei a rilevare lo stato di salute della popolazione previsto dai programmi di ricerca biomedica e sanitaria di cui all'art. 12-bis d.lgs 502/1992 e succ. modif.***	**NO**[20]	**SI,** ***gli scopi statistici o scientifici devono essere chiaramente determinati e resi noti all'interessa-to***[21]***.***	**SI** ***ove si tratti dati diversi da quelli identificati nella legge istitutiva.***	**NO**

[15] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante. Il titolare che abbia iniziato il trattamento anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che lo abbia notificato in passato, deve procedere, se vi è tenuto, entro il 30 aprile 2004 (art. 181, comma 1, lett. c).

[16] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice"). Il trattamento può essere iniziato se è decorso il termine di quarantacinque giorni dalla comunicazione al Garante.

[17] L'identificazione è avvenuta con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni. ARS non ha potestà regolamentare, quindi è inserita nell'ambito del regolamento privacy della Regione Toscana. Nello specifico con la pubblicazione sul BURT n. 7 del 15 febbraio 2013, Parte Prima, del DECRETO DEL PRESIDENTE DELLA GIUNTA REGIONALE 12 febbraio 2013, n. 6/R è entrato in vigore il " Regolamento di attuazione dell´articolo 1, comma 1, della legge regionale 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)". L'emanazione del presente Regolamento ha comportato la contestuale abrogazione del precedente regolamento di pari oggetto (DPRG 18/R/2006). La disciplina per ARS è inserita nella scheda n. 12 Allegato A) (cfr. artt. 20 e 181 "Codice").

[18] L'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio.

19 Il trattamento di dati sensibili per scopi statistici o scientifici è soggetto alla disciplina del Codice di deontologia e di buona condotta di cui all'art. 106 "Codice".

20 Quando la ricerca è prevista da espressa disposizione di legge (ed è il caso dell'ARS), ovvero rientra in un programma di ricerca biomedica e sanitaria previsto dall'art. 12- bis d.lgs. 502/1992 e successive modificazioni.

[21] L'informativa all'interessato non è dovuta quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate nei Codici di deontologia e di buona condotta (Art. 105, c. 4 e Art. 106 "Codice").

TIPOLOGIA	AUTORIZ-ZAZIONE GARANTE (Art. 18 e 19)	COMUNICA-ZIONE AL GARANTE (Artt. 19, co. 2 e 39, co. 1, lett. a)	CONSENSO INTERES-SATO (Art.18)	INFORMATI-VA INTERES-SATO (Art.13)	REGOLAMEN-TO DATI (Art.19)[22]	DOCU-MENTO PROGRAM-MATICO SICUREZZA (Art. 34, co. 1, lett. g) e All. B)[23]	COMUNICAZIO-NE TRA ENTI PUBBLICI (Art. 19)
ENTE PUBBLICO Trattamento dati comuni (ovvero diversi da quelli sensibili)[24]	**NO**	**SI**, ***nel caso di comunicazione di dati personali da parte di un soggetto pubblico all'ARS e viceversa, non previsto da norma di legge o regolamento, effettuata in qualsiasi forma anche mediante convenzione[25].***	**NO**	**SI**	**NO**	**NO**	**SI,** ***circa la comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico prevista da norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento delle funzioni istituzionali. La comunicazione da parte di un soggetto pubblico a privati o ad enti pubblici economici e la diffusione sono ammessi solo se previste da legge o regolamento.***

[22] L'identificazione è avvenuta con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni. ARS non ha potestà regolamentare, quindi è inserita nell'ambito del regolamento privacy della Regione Toscana. Nello specifico con la pubblicazione sul BURT n. 7 del 15 febbraio 2013, Parte Prima, del DECRETO DEL PRESIDENTE DELLA GIUNTA REGIONALE 12 febbraio 2013, n. 6/R è entrato in vigore il " Regolamento di attuazione dell´articolo 1, comma 1, della legge regionale 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)". L'emanazione del presente Regolamento ha comportato la contestuale abrogazione del precedente regolamento di pari oggetto (DPRG 18/R/2006). La disciplina per ARS è inserita nella scheda n. 12 Allegato A). (cfr. artt. 20 e 181 "Codice").

[23] L'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio.

[24] Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

[25] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione, oppure mediante telefax o lettera raccomandata (artt. 19, co. 2 e 39. comma 1, lett. a) e co. 2, "Codice"). Il trattamento può essere iniziato se è decorso il termine di quarantacinque giorni dalla comunicazione al Garante.

ALLEGATO 2

OBBLIGHI SOGGETTI

TAV. 1

TITOLARE	▪ **Nominare uno o più responsabili in relazione all'esigenza organizzativa dell'Ente; i compiti attribuiti sono specificati analiticamente per iscritto unitamente ad istruzioni tecniche ivi compreso il profilo di sicurezza (cfr. art. 16, dir. 95/46/CE; art. 8, comma 1, l. n. 675/1996 ; art. 29 "Codice").** ▪ **Adottare ed aggiornare, su proposta dei Responsabili, il Documento programmatico sulla sicurezza (da artt. 33 a 35 e all. B "Codice")[26].** ▪ **Identificare con atto di natura regolamentare, su proposta dei Responsabili, i tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni nonché la disciplina dei rapporti con enti di altre regioni anche mediante convenzioni (cfr. artt. 20 e 181 "Codice")[27].** ▪ **Richiedere, su proposta dei Responsabili, l'autorizzazione al Garante per il trattamento di dati sensibili qualora l'Agenzia operi come organismo sanitari pubblico (cfr. art. 76 "Codice".** ▪ **Notificare al Garante, su proposta dei Responsabili, il trattamento di dati sensibili, sia si tratti di dati di tipo sanitario per perseguire finalità collettive , sia per il trattamento per scopi statistici o scientifici (cfr. artt. 37 e 38 "Codice")[28].** ▪ **Comunicare al Garante, su proposta dei Responsabili, il trattamento di dati idonei a rilevare lo stato di salute della popolazione, trattati a qualsiasi titolo, previsti dai programmi di ricerca biomedica e sanitaria di cui all'art. 12- bis d.lgs. 502/1992 e succ. modif. (cfr. art. 39, c.1. lett.b) "Codice")[29].** ▪ **Comunicare al Garante, su proposta dei Responsabili, i dati personali comunicati da parte di un soggetto pubblico all'ARS e viceversa, non previsti da norma di legge o regolamento, effettuata in qualunque forma anche mediante convenzione (cfr. art. 39, comma 1, lett. a) "Codice")[30].**

[26] L'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio.

[27] L'identificazione deve avvenire con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni (cfr. artt. 20 e 181 "Codice"). ARS non ha potestà regolamentare, quindi è inserita nell'ambito del regolamento privacy della Regione Toscana. Nello specifico con la pubblicazione sul BURT n. 7 del 15 febbraio 2013, Parte Prima, del DECRETO DEL PRESIDENTE DELLA GIUNTA REGIONALE 12 febbraio 2013, n. 6/R è entrato in vigore il " Regolamento di attuazione dell´articolo 1, comma 1, della legge regionale 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)". L'emanazione del presente Regolamento ha comportato la contestuale abrogazione del precedente regolamento di pari oggetto (DPRG 18/R/2006). La disciplina per ARS è inserita nella scheda n. 12 Allegato A)

[28] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante. Il titolare che abbia iniziato il trattamento anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che lo abbia notificato in passato, deve procedere, se vi è tenuto, entro il 30 aprile 2004 (art. 181, comma 1, lett. c).

[29] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice").

[30] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione, oppure mediante telefax o lettera raccomandata (artt. 19, co. 2 e 39. comma 1, lett. a) e co. 2, "Codice"). Il trattamento può essere iniziato se è decorso il termine di quarantacinque giorni dalla comunicazione al Garante.

TAV. 2

SOGGETTI	OBBLIGHI
RESPONSABILE	▪ **Applicare le istruzioni tecniche impartite dal Titolare.** ▪ **Nominare uno o più incaricati in relazione alle esigenze organizzative dell'ente; i compiti attribuiti sono specificati analiticamente per iscritto unitamente alle istruzioni tecniche.** **I Responsabili, inoltre, collaborano con il Titolare per la privacy provvedendo a:** ▪ **fornire le informazioni richieste;** ▪ **metterlo a conoscenza, tempestivamente, di tutte le questioni rilevanti ai fini del d.lgs. 196/2003;** ▪ **comunicare l'inizio di ogni nuovo trattamento nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di competenza ai fini dell'aggiornamento dell'anagrafe dei trattamenti di dati personali dell'ARS;** ▪ **disporre per la tenuta ed aggiornamento del censimento dei trattamenti dei dati sensibili e/o personali, anche ai fini dell'adozione delle altre misure di sicurezza, e per l'eventuale adozione da parte del titolare di un atto di natura regolamentare con il quale s'identifichino i tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni nonché la disciplina dei rapporti con enti di altre regioni anche mediante convenzioni (cfr. artt. 20 e 181 "Codice")**[31]**.** ▪ **proporre le misure di sicurezza, ivi compresa l'analisi dei rischi e delle contromisure da adottare, nonché la pianificazione degli interventi formativi, ai fini dell'adozione e dell'aggiornamento delle altre misure di sicurezza**[32]**;** ▪ **proporre istanza di autorizzazione al Garante, per il trattamento di dati sensibili qualora l'Agenzia operi come organismo sanitario pubblico (cfr. art. 76 "Codice");** ▪ **proporre di notificare al Garante il trattamento di dati sensibili, sia si tratti di dati di tipo sanitario per perseguire finalità collettive, sia per il trattamento per scopi statistici o scientifici (cfr. artt. 37 e 38 "Codice")**[33]**;** ▪ **proporre di comunicare al Garante il trattamento di dati idonei a rilevare lo stato di salute della popolazione previsti dai programmi di ricerca biomedica e sanitaria di cui all'art. 12- bis d.lgs. 502/1992 e succ. modif. (cfr. art. 39, c.1. lett. b), Codice")**[34]**.** ▪ **Proporre al titolare di comunicare al Garante i dati personali comunicati da parte di un soggetto pubblico all'ARS e viceversa, non previsto da norma di legge o regolamento, effettuata in qualunque forma anche mediante convenzione (cfr. art. 39, comma 1, lett. a) "Codice").**[35]

[31] L'identificazione deve avvenire con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni (cfr. artt. 20 e 181 "Codice"). ARS non ha potestà regolamentare, quindi è inserita nell'ambito del regolamento privacy della Regione Toscana. Nello specifico con la pubblicazione sul BURT n. 7 del 15 febbraio 2013, Parte Prima, del DECRETO DEL PRESIDENTE DELLA GIUNTA REGIONALE 12 febbraio 2013, n. 6/R è entrato in vigore il " Regolamento di attuazione dell´articolo 1, comma 1, della legge regionale 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)". L'emanazione del presente Regolamento ha comportato la contestuale abrogazione del precedente regolamento di pari oggetto (DPRG 18/R/2006). La disciplina per ARS è inserita nella scheda n. 12 Allegato A) (cfr. artt. 20 e 181 "Codice").

[32] L'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio.

[33] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante. Se il trattamento è iniziato anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che sia stato notificato in passato, si deve procedere, ove tenuti, entro il 30 aprile 2004 (art. 181, comma 1, lett. c).

[34] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice").

TAV. 3

SOGGETTI	OBBLIGHI
INCARICATO	▪ **Esegue il trattamento sulla base delle prescrizioni tecniche emanate dai Responsabili.** ▪ **Coadiuva il Responsabile:** ➢ **nella tenuta ed aggiornamento del censimento dei trattamenti dei dati personali e/o sensibili, anche ai fini dell'adozione del Documento programmatico della sicurezza, e per l'eventuale adozione da parte del Titolare di un atto di natura regolamentare con il quale si identifichino i tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni nonché la disciplina dei rapporti con enti di altre regioni anche mediante convenzioni (cfr. artt. 20 e 181 "Codice")[36]..** ➢ **per proporre al Titolare le misure di sicurezza, ivi compresa l'analisi dei rischi e delle contromisure da adottare, ai fini dell'adozione e dell'aggiornamento del Documento programmatico della sicurezza[37].** ➢ **per proporre al Titolare istanza di autorizzazione al Garante, per il trattamento di dati sensibili qualora l'Agenzia operi come organismo sanitari pubblico (cfr. art. 76 "Codice".** ➢ **per proporre al titolare di notificare al Garante il trattamento di dati sensibili, sia si tratti di dati di tipo sanitario per perseguire finalità collettive, sia per il trattamento per scopi statistici o scientifici (cfr. artt. 37 e 38 "Codice")[38].** ➢ **per proporre al Titolare di comunicare al Garante il trattamento di dati idonei a rilevare lo stato di salute della popolazione previsti dai programmi di ricerca biomedica e sanitaria di cui all'art. 12- bis d.lgs. 502/1992 e succ. modif. (cfr. art. 39, c. 1,. lett.b) "Codice")[39].** ➢ **per proporre al Titolare di comunicare al Garante i dati personali comunicati da parte di un soggetto pubblico all'ARS e viceversa, non previsto da norma di legge o regolamento, effettuata in qualunque forma anche mediante convenzione (cfr. art. 39, comma 1, lett. a) "Codice") [40]**

[35] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione, oppure mediante telefax o lettera raccomandata (artt. 19, co. 2 e 39. comma 1, lett. a) e co. 2, "Codice"). Il trattamento può essere iniziato se è decorso il termine di quarantacinque giorni dalla comunicazione al Garante.

[36] L'identificazione con atto di natura regolamentare dei tipi di dati trattati non previsti dalla legge istitutiva e delle relative operazioni, deve essere adottato entro il 30 settembre 2004 (cfr. artt. 20 e 181 "Codice").

[37] L'art. 45 del D.L. 9 febbraio 2012, n. 5 ("Disposizioni urgenti in materia di semplificazione e sviluppo", altrimenti noto come "Decreto semplificazioni") cancella l'obbligo di redazione a. aggiornamento del Documento programmatico sulla sicurezza ("DPS") ed elimina anche l'obbligo collaterale di dare atto della sua approvazione/aggiornamento nella relazione accompagnatoria al bilancio di esercizio

[38] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante. Se il trattamento è iniziato anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che sia stato notificato in passato, si deve procedere, ove tenuti, entro il 30 aprile 2004 (art. 181, comma 1, lett. c).

[39] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice").

[40] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione, oppure mediante telefax o lettera raccomandata (artt. 19, co. 2 e 39. comma 1, lett. a) e co. 2, "Codice"). Il trattamento può essere iniziato se è decorso il termine di quarantacinque giorni dalla comunicazione al Garante.

Allegato B

CLAUSOLA DI GARANZIA PER TRATTAMENTO DI DATI DA PARTE DI SOGGETTI ESTERNI ALL'ARS.

L'Azienda o Ditta _____ alla quale l'ARS ha affidato con _____del _____l'attività di _____e corresponsabile con l'Agenzia stessa del trattamento di dati relativi al trattamento _____ censito nel CETRA dell'Agenzia al n°_____.

Nell'effettuare le operazioni e i compiti affidati e nel rispetto del disciplinare sulla sicurezza, la stessa dovrà osservare le norme di legge sulla protezione dei dati personali ed attenersi alle decisioni del Garante dei dati personali e dell'Autorità giudiziaria, provvedendo ad evaderne le richieste. L'Azienda/Ditta è altresì tenuta ad osservare compiutamente quanto disposto dall'Agenzia nel rispetto della disciplina di cui alla d.lgs. n. 196/2003 e ss.mm. ed in particolare dovrà informare l'ARS della puntuale adozione di tutte le misure di sicurezza disposte dal documento programmatico sulla sicurezza, così da evitare rischi di distruzione e perdita,anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. In ogni caso l'Azienda/Ditta si impegna espressamente a non effettuare operazioni di comunicazione e diffusione dei dati personali sottoposti al trattamento verso soggetti terzi diversi dall'Agenzia committente senza preventivo consenso dell'ARS stessa, non rientrando tali operazioni tra quelle affidate alla medesima.

Allegato C

NOTIFICA AL GARANTE

Vedi sito: www.garanteprivacy.it (la nuova notificazione)

Allegato D

IPOTESI DI INFORMATIVA

Informativa per il trattamento di dati personali
Art. 13 decreto legislativo 30 giugno 2003, n. 196
"Codice in materia di protezione dei dati personali"

Ai sensi del D.lgs. n.196/2003 (codice relativo al trattamento dei dati personali), il trattamento dei dati personali sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della riservatezza e dei diritti degli interessati.

Ai sensi dell'articolo 13 del Codice L'ARS dichiara quanto segue:

a) Il trattamento dei dati personali viene effettuato dall'ARS, come stabilito dalla legge istitutiva legge regionale 24 febbraio 2005, n. 40 "Disciplina del Servizio sanitario regionale" e ss.mm. , per le seguenti finalità: .....

b) Il trattamento sarà effettuato con le seguenti modalità: .....(Indicare le modalità del trattamento: manuale / informatizzato / altro.)

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

d) I dati non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione

o

i dati potranno essere / saranno comunicati a: ..... o diffusi presso: .....*(Scegliere l'opzione a seconda delle caratteristiche del trattamento ed indicare, se presente, l'ambito di comunicazione e/o diffusione, fermo restando il divieto relativo ai dati idonei a rivelare lo stato di salute, di cui all'art. 22, comma 8 del Codice).*

e) Il titolare del trattamento è: ..... (Indicare denominazione e indirizzo del titolare)

f) I responsabili del trattamento sono ..... (Indicare denominazione e indirizzo dei responsabili)

g) Ogni interessato potrà rivolgersi al titolare del trattamento o ai responsabili per far valere i propri diritti, così come previsto dall'articolo 7 del D.lgs n.196/2003 e ss.mm.;

h) per facilitarne l'esercizio da parte dell'interessato sono di seguito riportati i diritti ex art. 7 del Codice e sono illustrate le modalità per il loro esercizio:

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

3. L'interessato ha diritto di ottenere l'indicazione:
   a. dell'origine dei dati personali;

   b. delle finalità e modalità del trattamento;
   c. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d. degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

4. L'interessato ha diritto di ottenere:
   a. l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

   b. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

5. L'interessato ha diritto di opporsi, in tutto o in parte:
   a. per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b. al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale."

Si potranno esercitare tali diritti inviando una e-mail a ……, un fax al numero……, o una lettera raccomandata all'indirizzo ……

Allegato E

MODELLO NOMINA INCARICATI

Firenze, ……
Prot. n. ……..

Oggetto: Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) ss.mm. – Nomina degli incaricati dei trattamenti di dati personali di competenza del f.f. Coordinatore Osservatorio di epidemiologia e del Coordinatore Osservatorio per la Qualità e l'Equità – (*Nome Cognome incaricato*)

I RESPONSABILI AL TRATTAMENTO DEI DATI AFFERENTI ALL'OSSERVATORIO DI EPIDEMIOLOGIA E OSSERVATORIO PER LA QUALITÀ E L'EQUITÀ

Vista la legge regionale 24 febbraio 2005, n. 40 (*Disciplina del servizio sanitario regionale*) e successive modificazioni ed integrazioni;

Visto il decreto legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali"* e ss.mm., di seguito nominato "Codice"e relative disposizioni attuative del Garante;

Richiamato, in particolare, l'art. 29 del medesimo Codice che disciplina la figura del responsabile del trattamento dei dati, definendone compiti e responsabilità;

Considerato che la normativa citata sottopone le pubbliche amministrazioni ad uno speciale regime giuridico, finalizzato ad assicurare la tutela della riservatezza e la protezione dei dati personali in relazione ai trattamenti che avvengono in ambito pubblico;

Vista la citata legge regionale. 24 febbraio 2005, n. 40 e specificatamente, l'art. 82-*duodecies* della stessa, con cui si definiscono le strutture organizzative dell'ARS;

Preso atto del decreto del presidente della Giunta regionale 12 febbraio 2013, n. 6/R recante "*Regolamento di attuazione dell'articolo 1, comma 1, della legge regionale 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)*";

Visto altresì il decreto del direttore n. 48 del 16/09/2014, con cui si è proceduto a nominare, in attuazione degli articoli 28 e 29 del richiamato Codice, quali Responsabili del trattamento dati personali il coordinatore dell'osservatorio di epidemiologia per i trattamenti afferenti all'osservatorio di competenza e il coordinatore dell'osservatorio per la qualità e l'equità per i trattamenti afferenti all'osservatorio di competenza, impartendo loro specifiche istruzioni, ivi compreso il profilo di sicurezza;

Considerato che a partire dal …….. fino al …….. è stato attivato un progetto denominato …….. presso …… (indicare settore /osservatorio), avente ad oggetto lo svolgimento dell'attività di ….……..;

Visto che per lo svolgimento dell'attività relativa al sopra progetto citato, il dott./la dott.ssa …… dovrà accedere ad alcuni flussi, nello specifico:

- …….
- …….
- …….
- …….

Ritenuto opportuno procedere ai sensi dell'art. 30 del più volte citato Codice, nell'ambito dell'attività di cui ai paragrafi che precedono, alla nomina quale incaricato dei trattamenti di dati personali di:

- ***Nome e Cognome nato/a a …….. il ……., incaricato esterno;***

oppure

- ***Nome e Cognome ……..incaricato interno***

identificato nell'elenco allegato sub. lett. "A", parte integrante e sostanziale del presente provvedimento, in cui sono individuati i profili di autorizzazione e, quindi, le operazioni eseguibili, nonché l'ambito del trattamento consentito (per le operazioni svolte da ciascun incaricato per propria competenza), fornendo le specifiche istruzioni di cui all'Allegato sub. lett. "B", parte integrante e sostanziale del presente atto, che recepiscono i contenuti essenziali della richiamata direttiva regionale, adeguandoli alle esigenze organizzative dell'Ente;

Ritenuto altresì di precisare che nel richiamato allegato sub. lett. A i nominativi degli incaricati contrassegnati con un asterisco sono nominati d'intesa tra il responsabile del trattamento dati del settore amministrazione e il responsabile dell'osservatorio indicato; gli incaricati contrassegnati con doppio asterisco sono nominati d'intesa tra i due responsabili delle strutture organizzative di ARS;

DISPONGONO

1. di nominare quale incaricato dei trattamenti di dati personali, ai sensi dell'art. 30 del più volte citato Codice, nell'ambito dell'attività/progetto ……., avente ad oggetto ……:

   Nome e Cognome nato/a a ……. il ……., incaricato interno/ esterno;

   identificato nell'elenco allegato sub. lett. "A", parte integrante e sostanziale del presente provvedimento, in cui sono individuati i profili di autorizzazione e, quindi, le operazioni eseguibili, nonché l'ambito del trattamento consentito (per le operazioni svolte da ciascun incaricato per propria competenza);

2. di impartire le prescrizioni contenute nell'allegato sub. lett. "B", parte integrante del presente atto, che recepiscono i contenuti essenziali del richiamato decreto del presidente della Giunta regionale 12 febbraio 2013, n. 6/R, adeguandoli alle esigenze organizzative dell'Ente;

3. di stabilire che l'incaricato al trattamento, così come identificato al punto 1, deve attenersi scrupolosamente alle prescrizioni di cui al punto 2.

Il f.f. Coordinatore
dell'Osservatorio di Epidemiologia
(dr. Fabio Voller)

Il Coordinatore
dell'Osservatorio per la Qualità e l'equità
(dr. Andrea Vannucci)

All. n. 2

Per presa visione

……..