Gruppo di redazione: Simona Gallo, Gianni Amunni, Riccardo Poli, Fabrizio Carraro

	NOME	FUNZIONE	DATA	FIRMA
REDAZIONE	Simona Gallo	Settore Affari Generali e Convenzioni	03/09/2015	
VERIFICA	Fabrizio Carraro	Direttore Amministrativo	" " "	
APPROVAZIONE	Gianni Amunni	Direttore Generale	05/09/2015	

INDICE

1. SCOPO

2. CAMPO DI APPLICAZIONE

3. RIFERIMENTI

4. QUADRO NORMATIVO
   - 4.1 IL DIRITTO ALLA PRIVACY E LA DIRETTIVA 95/46/CE
   - 4.2 IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (D.LGS. 30 GIUGNO 2003, N. 196)
   - 4.3 REGOLAMENTI SUL TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI
   - 4.4 NORMATIVE DI SETTORE

5. NOZIONI ED ISTRUZIONI DI CARATTERE GENERALE
   - 5.1 DATI PERSONALI E DATI ANONIMI
   - 5.2 TRATTAMENTO DI DATI PERSONALI
   - 5.3 PRINCIPI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI
   - 5.4 I SOGGETTI CONNESSI ALLA PROTEZIONE DEI DATI PERSONALI
   - 5.5 L'INTERESSATO
   - 5.6 INFORMATIVA ALL'INTERESSATO
   - 5.7 DIRITTO DI ACCESSO AI DATI DA PARTE DELL'INTERESSATO
   - 5.8 CONSENSO DELL'INTERESSATO
   - 5.9 TITOLARE DEL TRATTAMENTO
   - 5.10 CONTITOLARITÀ DEL TRATTAMENTO
   - 5.11 RESPONSABILI DEL TRATTAMENTO
   - 5.12 RESPONSABILI ESTERNI DEL TRATTAMENTO
   - 5.13 INCARICATO DEL TRATTAMENTO
   - 5.14 FORMAZIONE DEGLI INCARICATI
   - 5.15 REFERENTE AZIENDALE PER LA PRIVACY
   - 5.16 INCARICATO DEL TRATTAMENTO "AMMINISTRATORE DI SISTEMA"
   - 5.17 L'ATTIVITÀ NORMATIVA DELL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
   - 5.18 OBBLIGHI DI NOTIFICAZIONE AL GARANTE
   - 5.19 OBBLIGHI DI COMUNICAZIONE AL GARANTE
   - 5.20 MISURE DI SICUREZZA MINIME E IDONEE
   - 5.21 SANZIONI

6. DEFINIZIONI

DISTRIBUZIONE

La presente procedura viene distribuita ai Responsabili delle seguenti Strutture o Centri di Responsabilità che, a loro volta, provvedono a distribuirla e, ove occorra, ad illustrarla al personale interessato appartenente alla propria struttura

		Si/No
Direzione Generale		Si
Direzione Sanitaria		Si
Direzione Amministrativa		Si
Coordinamento Assistenziale e di Prevenzione		Si
Coordinamento Tecnico-sanitario		Si
Coordinamento Statistico		Si
S.S. Contabilità e Controllo di Gestione		Si
S.S. Formazione, Attività Editoriali e Comunicazione		Si
S.S. Centro Riabilitazione Oncologica		Si
STRUTTURE COMPLESSE	STRUTTURE SEMPLICI COLLEGATE	Si
Laboratorio di Prevenzione Oncologica	Diagnostica HPV e Oncologia Molecolare	Si
	Citologia extrascreening	
Senologia		Si
Prevenzione Secondaria - Screening	Mammografia Screening	Si
	CRR Prevenzione Oncologica	
Epidemiologia Clinico-Descrittiva e Registri	Infrastruttura Registri	Si
	Valutazione Screening	
Epidemiologia Molecolare Nutrizionale		Si
Biostatistica Applicata	Epidemiologia Ambientale ed Occupazionale	Si
Gestione Coordinamento Processi e Integrazione Aree Amministrativa e Tecnico-scientifica e Supporto Amministrativo ITT		Si

1. SCOPO

Il presente documento intende offrire una ricognizione generale dei principi e delle norme vigenti in materia di Privacy e definire le figure e gli strumenti di carattere organizzativo per l'applicazione delle disposizioni del D.Lgs. 30 giugno 2003, n.196 Codice in materia di protezione dei dati personali, al fine di assicurare 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" (art. 2).

2. CAMPO DI APPLICAZIONE

Il presente documento si rivolge a tutti i soggetti, dipendenti e non, compresi i soggetti con incarico libero professionale o altro personale non strutturato, che effettuano, anche a titolo volontario (ove non incaricati all'uopo dalla Associazione di appartenenza che intrattenga specifici rapporti convenzionali con ISPO), operazioni di trattamento dei dati personali per conto di ISPO.
Al presente documento, che contiene nozioni e istruzioni di carattere generale, faranno richiamo espresso i successivi documenti redatti e adottati per la gestione dei singoli ambiti settoriali (Nozioni e istruzioni generali in materia di trattamento di dati personali per la gestione del rapporto di lavoro; Nozioni e istruzioni generali in materia di trattamento dei dati personali in ambito sanitario, ecc).

3. RIFERIMENTI

- *Direttiva del Parlamento Europeo e del Consiglio 95/46/CE del 24 ottobre 1995*, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali
- *D. Lgs. 196 del 30 giugno 2003 Codice in materia di protezione dei dati personali* e successive modifiche ed integrazioni, compreso il relativo Allegato B Disciplinare tecnico in materia di misure minime di sicurezza
- *Dipartimento della Funzione Pubblica - Direttiva 1/2005* Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196, con particolare riguardo alla gestione delle risorse umane.

Regione Toscana:
- Delibera Giunta Regionale 29 novembre 2004 Linee guida alle Aziende sanitarie per l'applicazione del D. Lgs. 196 del 30 giugno 2003 Codice in materia di protezione dei dati personali
- Decreto del Presidente della Giunta regionale 16 maggio 2006: Regolamento per il 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
- Delibera Giunta regionale 12 marzo 2007 n. 167 Direttiva per l'attuazione del Decreto Legislativo n. 196/2003 recante "Codice in materia di protezione dei dati personali".

Autorità Garante per la Protezione dei dati personali:
- Provvedimento Strutture sanitarie: rispetto della dignità - 9 novembre 2005
- Provvedimento Internet: proporzionalità nei controlli effettuati dal datore di lavoro - 2 febbraio 2006
- Autorizzazione al trattamento dei dati genetici - 22 febbraio 2007
- Provvedimento Lavoro: le linee guida del Garante per posta elettronica e internet - 1 marzo 2007

- Provvedimento Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico - 14 giugno 2007
- Provvedimento Limiti al controllo sulla posta elettronica del dipendente - 2 aprile 2008
- Provvedimento Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008
- Provvedimento Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008
- Provvedimento Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008
- Provvedimento Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 12 febbraio 2009
- Provvedimento Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009
- Provvedimento Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009
- Provvedimento Linee guida in tema di referti on-line - 19 novembre 2009
- Autorizzazione per uno studio epidemiologico di pazienti oncologici, senza consenso informato - 16 aprile 2009
- Provvedimento in materia di videosorveglianza - 8 aprile 2010
- Ulteriore differimento dell'efficacia dell'autorizzazione al trattamento dei dati genetici, rilasciata il 22 febbraio 2007 - 23 dicembre 2010
- Provvedimento Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web - 2 marzo 2011
- Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - 11 dicembre 2014
- Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica - 11 dicembre 2014.

4. QUADRO NORMATIVO

4.1 IL DIRITTO ALLA PRIVACY E LA DIRETTIVA 95/46/CE

Le normative attualmente vigenti nei vari Stati Europei, in applicazione della Direttiva del Parlamento Europeo e del Consiglio 95/46/CE del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, inquadrano e sostengono tale diritto attraverso una difesa più estesa, commisurata alle esigenze ed ai rischi della attuale società dell'informazione. Tende così a prevalere una definizione di diritto alla privacy che fa riferimento alla possibilità di un soggetto (il c.d. Interessato) di conoscere e controllare il flusso di informazioni che lo riguardano.

4.2 IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (D.LGS. 30 GIUGNO 2003, N. 196)

Il Decreto Legislativo 30 giugno 2003 n. 196 Codice in materia di protezione dei dati personali rappresenta oggi, nel nostro ordinamento, il testo normativo di riferimento in materia di tutela della riservatezza (o meglio di protezione dei dati personali). Esso garantisce "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" (art. 2). Il diritto alla protezione dei dati personali riconosciuto dal Codice è, quindi, un diritto che si può ricomprendere tra i diritti e le libertà fondamentali ed è qualificabile, più precisamente, come un diritto della personalità (quali il diritto alla vita, alla salute, alla libertà sessuale, all'identità personale, all'onore, alla reputazione al nome, morale d'autore ecc.), funzionale alla tutela della dignità dell'interessato sia in termini di riservatezza (intesa come il diritto alla segretezza ed alla intimità della vita privata, in relazione a comunicazioni, comportamenti, immagini) che di identità personale (il "diritto ad essere sé stesso", a non veder travisato il proprio patrimonio intellettuale, politico, religioso, sociale). Tale diritto viene perciò riconosciuto anche allo straniero, ovvero al cittadino non comunitario (cfr. anche l'art. 2 comma 1 del d. Lgs. 25 luglio 1998, n. 286 Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, che riconosce "i diritti fondamentali della persona umana" allo straniero "comunque presente alla frontiera o nel territorio dello Stato").

4.3 REGOLAMENTI SUL TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI

I regolamenti sul trattamento dei dati sensibili e giudiziari, adottati ai sensi dell'art. 20 del Codice rappresentano una fonte normativa basilare per definire la liceità e la correttezza di un determinato trattamento. Infatti, relativamente al trattamento di dati sensibili e giudiziari, qualora manchi una previsione di legge che identifichi i dati trattabili e le operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare, adottato in conformità al parere espresso dal Garante. Tale Regolamento, per le aziende del Servizio Sanitario Toscano (prive di autonoma potestà regolamentare esterna) è stato adottato da Regione Toscana con Decreto del Presidente della Giunta regionale 16 maggio 2006 Regolamento per il 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.

4.4 NORMATIVE DI SETTORE

Restano in vigore alcune normative di settore (es. osservanza segreto professionale, tutela della dignità del paziente, soprattutto con riguardo a fasce deboli (disabili, minori, anziani), la riservatezza nei colloqui e delle informazioni sulla salute, sulle prescrizioni mediche e sulle cartelle cliniche), che si affiancano al Codice, nel loro ambito specifico, nella definizione dei requisiti di legittimazione dei relativi trattamenti.

5. NOZIONI ED ISTRUZIONI DI CARATTERE GENERALE

5.1 DATI PERSONALI E DATI ANONIMI

Ai sensi dell'art. 4 comma 1 b) del Codice è **dato personale**:
qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
E' dunque anzitutto dato personale "qualunque informazione", nel senso di qualunque tipologia di informazione, sia essa testo scritto, immagine, suono ecc.; per esemplificare, sono stati via via qualificati dal Garante come dato personale:
- la registrazione della voce di un soggetto (ad es. le chiamate registrate dal 118);
- le immagini filmate da un impianto di videosorveglianza, nella misura in cui i singoli individui siano riconoscibili;
- l'indirizzo Ip di posta elettronica;
- l'impronta digitale, ovvero un dato biometrico, che è dato personale in quanto identifica una persona (laddove i campioni di tessuto dai quali si estraggono i dati biometrici non sono di per sé dati personali, anche se le operazioni effettuate per estrarre tali informazioni biometriche configurano già un trattamento di dati personali);
- il disegno dei familiari da parte di un paziente nell'ambito di un test neuropsichiatrico, che si traduce in "dato personale" in quanto, offrendo informazioni sul suo stato d'animo e sui suoi sentimenti per i diversi membri della famiglia, rivela informazioni sulla salute mentale del soggetto (ed eventualmente anche sul comportamento dei familiari).

Dato anonimo, cioè non personale, secondo l'art. 4 comma 1 n del Codice è:
il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
Dalla sopra richiamata definizione di dati personali si evidenzia inoltre un'articolazione *("identificati o identificabili, anche indirettamente")* tra:
- dati personali identificativi, ovvero dati che permettono l'identificazione diretta dell'interessato (es. nome/cognome, impronta digitale), nel senso che permettono di stabilire direttamente una correlazione più o meno univoca tra un soggetto ed alcune informazioni che lo riguardano;
- dati personali non immediatamente identificativi, ovvero che, per la identificazione di un soggetto, necessitano del riferimento ad altre informazioni (tali sono ad es. il numero di targa, il numero di telefono, il numero di matricola, i codici alfanumerici utilizzati nelle sperimentazioni); la correlazione in questi casi non è dunque immediata, ma è recuperabile in seconda istanza utilizzando altre informazioni.

5.2 TRATTAMENTO DI DATI PERSONALI

Quando si parla di trattamento dei dati personali, ai sensi dell'art. 4 comma 1 a) del Codice, ci si riferisce a:
qualunque operazione o complesso di operazioni 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.
Si ha trattamento di dati anche quando le suddette operazioni:
- siano effettuate senza l'ausilio di strumenti elettronici,

- riguardino dati non registrati in banche di dati (ovvero dati conservati in archivi non organizzati).

Dal punto di vista dei soggetti, la nozione di trattamento pone una correlazione obbligatoria almeno tra due figure: da un lato il **titolare**, ovvero il soggetto che, avvalendosi di **responsabili e incaricati**, organizza il trattamento; dall'altro l'**interessato**, il soggetto al quale i dati trattati si riferiscono.

Dal punto di vista strutturale, il trattamento dei dati è sostanzialmente un processo, caratterizzato dalle seguenti operazioni:

- una fase di input, ovvero di raccolta e registrazione dei dati, tramite loro acquisizione dall'interessato o presso terzi;
- una fase di operazioni interne: organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, cancellazione e distruzione di dati;
- una eventuale fase di output, ovvero di comunicazione o diffusione dei dati stessi.

Dalla definizione normativa di trattamento sopra richiamata si inferisce che il trattamento dei dati inizia fin dalla fase della raccolta delle informazioni e non riguarda la sola fase di elaborazione e comunicazione/diffusione; da cui l'obbligo ad es. che l'informativa che deve normalmente essere preventiva, sia appunto data prima della raccolta stessa dei dati.

Il trattamento di dati personali è ammesso solo da parte del titolare, dei responsabili e degli incaricati; l'Istituto non consente il trattamento di dati da parte di personale non individuato e legittimato, a pena di incorrere in un trattamento illegittimo passibile di sanzioni.

5.3 PRINCIPI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

Il Codice, all'art. 11, stabilisce che i dati personali devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- esatti e, se necessario, aggiornati;
- 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.

In sintesi, per soddisfare il principio di liceità il trattamento dei dati deve rispettare:

- presupposti e limiti stabiliti dal Codice, dalle leggi, dai regolamenti e dalle disposizioni dell'Autorità Garante;
- eventuali disposizioni contenute nei codici di deontologia e di buona condotta di cui all'allegato A del Codice, promossi dal Garante per determinati settori;
- misure minime di sicurezza di cui agli artt. 31-36 del Codice;
- normative di settore (es. osservanza segreto professionale, tutela della dignità del paziente, soprattutto con riguardo a fasce deboli (disabili, minori, anziani), la riservatezza nei colloqui e delle informazioni sulla salute, sulle prescrizioni mediche e sulle cartelle cliniche).

I dati sono trattati correttamente se il trattamento è svolto con la consapevolezza dell'interessato; da ciò consegue l'obbligo di una informativa che sia idonea (attraverso l'utilizzo di una terminologia comprensibile e al tempo stesso esaustiva) a rendere l'interessato convenientemente edotto dei

trattamenti dei dati che lo riguardano (l'inidoneità o addirittura l'omissione dell'informativa sono specificamente sanzionate).
Per ogni trattamento occorre una finalità determinata (cioè stabilita a priori), presente ed attuale (cioè tuttora valida), esplicita (cioè resa conoscibile) e lecita, la quale costituisce il parametro di riferimento per valutare i dati da trattare, sia in termini qualitativi che quantitativi. Le operazioni di trattamento non devono essere incompatibili con tali finalità (c.d. principio di finalità). E' ad es. legittimo il trattamento effettuato da parte del datore di lavoro delle informazioni relative all'appartenenza sindacale del dipendente per la gestione delle trattenute in busta paga; non lo sarebbe evidentemente allo scopo di discriminarlo.
Per gli enti pubblici tali finalità devono essere utili a soddisfare i rispettivi scopi istituzionali, nel senso che un ente pubblico non può effettuare trattamenti che non rientrino tra le proprie finalità istituzionali.
In particolare, per assicurare maggiori garanzie agli interessati, i trattamenti di dati sensibili e giudiziari effettuati da un ente pubblico sono leciti solo se riferibili a finalità di rilevante interesse pubblico individuate dalla legge. Quando la finalità è raggiunta o diviene irraggiungibile è necessario provvedere alla cancellazione o alla trasformazione in forma anonima dei dati, fatte salve le disposizioni in materia di archiviazione e conservazione dei documenti amministrativi. Ciò consente, tra l'altro, di prevenire possibili accessi abusivi ad informazioni non più attuali. E' considerato compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati l'ulteriore trattamento per fini storici, di ricerca scientifica o di statistica.
Il principio di pertinenza e non eccedenza sancisce l'obbligo di assicurare la proporzionalità tra mezzi impiegati e fini perseguiti, raccogliendo solo i dati strettamente funzionali e necessari per il raggiungimento degli scopi legittimi perseguiti, completi e non eccessivi rispetto agli scopi stessi. Per il c.d. principio di necessità, invece, devono essere applicate ai dati modalità di trattamento che permettano appunto di identificare l'interessato solo in caso di necessità. Il Codice prescrive dunque all'art. 3 di:
- ridurre al minimo l'utilizzazione di dati personali ed identificativi;
- non utilizzare dati personali se è possibile utilizzare dati anonimi;
- se occorre utilizzare dati personali, utilizzare dati personali identificativi solo quando necessario.

In accordo a tale principio i sistemi informativi debbono essere predisposti e configurati per ridurre al minimo l'uso di dati personali ed identificativi, specie quando le finalità di trattamento possono essere raggiunte utilizzando dati anonimi. In particolare, qualora il dato sia trattato da un soggetto pubblico, la norma richiede che siano trattati i soli dati essenziali per lo svolgimento delle attività istituzionali e che siano svolte le sole operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito.
Quando il trattamento riguardi dati sensibili è legittimo solo l'utilizzo dei dati strettamente indispensabili (non meramente necessari). In particolare, in ambito sanitario, ai sensi dell'art. 85 comma 4 del Codice "l'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività (...) secondo il principio dell'indispensabilità dei dati di volta in volta trattati".

5.4 I SOGGETTI CONNESSI ALLA PROTEZIONE DEI DATI PERSONALI

Le figure fondamentali connesse alla protezione dei dati personali sono: l'interessato, il titolare del trattamento, il responsabile, l'incaricato, il Referente aziendale per la privacy e il Garante.

5.5 L'INTERESSATO

L'interessato è il soggetto al quale i dati personali oggetto di trattamento si riferiscono: può essere tanto una persona fisica che persona giuridica, ente o associazione. La legge italiana tutela infatti anche i dati personali riferiti a persone giuridiche, enti o associazioni.

Variamente esemplificando, è dunque interessato, ai sensi del Codice, tanto il paziente che usufruisce dei servizi sanitari anche occasionalmente: es. visite ambulatoriali o prestazioni di diagnostica strumentale o di laboratorio, che il fornitore di beni o servizi, i cui dati sono trattati ai fini dell'espletamento del rapporto contrattuale (gestione ordini, gestione fatture, ecc.). Anche il dipendente viene naturalmente in considerazione come interessato in riferimento ai trattamenti di dati che lo riguardano per finalità di gestione del rapporto di lavoro.

All'interessato è riconosciuto il diritto di controllare che i trattamenti dei dati che lo riguardano siano effettuati lecitamente e correttamente e, in alcuni casi, solo se dal medesimo autorizzati; a tale scopo il Codice individua i seguenti strumenti:

- l'informativa;
- il diritto di accesso ai dati;
- il consenso (quando previsto).

5.6 INFORMATIVA ALL'INTERESSATO

L'interessato deve ricevere, antecedentemente o al momento della raccolta dei dati, una idonea informativa. L'informativa è la dichiarazione che il titolare o il responsabile del trattamento fornisce all'interessato relativamente all'utilizzo che intende fare delle informazioni che lo riguardano ed ai suoi diritti. Essa indica:

- le finalità per le quali e le modalità con le quali verranno trattati i dati;
- l'obbligatorietà o meno del conferimento dei dati da parte dell'interessato;
- le conseguenze di un eventuale rifiuto a fornire i dati;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o trasmessi (sulla distinzione tra comunicazione e trasmissione) e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'articolo all'art. 7 del Codice;
- il nominativo del Titolare e del Responsabile (o dei Responsabili).

5.7 DIRITTO DI ACCESSO AI DATI DA PARTE DELL'INTERESSATO

Ai sensi dell'art. 7 del Codice, l'interessato ha diritto di:

- conoscere, mediante accesso gratuito, l'esistenza di trattamenti di dati che possono riguardarlo;
- essere informato su:
    - il nome e il domicilio del Titolare e del Responsabile del trattamento;
    - le finalità e le modalità del trattamento;
    - l'eventuale ambito di comunicazione e diffusione;
- ottenere a cura del titolare o del responsabile, senza ritardo:

- 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.

L'interessato ha inoltre il diritto a:
- ottenere a cura del titolare o del responsabile, senza ritardo:
- 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;
- l'aggiornamento, la rettifica ovvero, qualora vi abbia interesse, l'integrazione dei dati;
- l'attestazione che le operazioni di cui sopra 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;
- opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

I diritti previsti dall'art. 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo; la richiesta può essere trasmessa anche mediante lettera raccomandata, fax, posta elettronica (o altro idoneo mezzo individuato dal Garante). In particolare, per quanto riguarda la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro comunicazione, l'interessato può avanzare richiesta anche oralmente (in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile).
Il riscontro alla richiesta da parte del titolare o del responsabile è fornito entro quindici giorni dal suo ricevimento. Se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato: in tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta.
I dati possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica. Tutte le istanze di accesso ex art. 7 del Codice sono comunicate al Referente aziendale per la privacy, che predispone il riscontro all'interessato; se la richiesta è relativa a dati sanitari, la comunicazione deve essere sottoscritta da parte di un medico.

5.8 CONSENSO DELL'INTERESSATO

I soggetti pubblici sono di norma autorizzati al trattamento dei dati senza il consenso dell'interessato con due rilevanti e decisive eccezioni nel caso di:
- trattamento di dati personali idonei a rivelare lo stato di salute per finalità di tutela della salute o dell'incolumità fisica dell'interessato (una più articolata modalità di legittimazione è prevista per i trattamenti di dati idonei a rilevare lo stato di salute per finalità di tutela della salute e dell'incolumità fisica di terzi o della collettività;

- trattamento finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico (sono previste alcune eccezioni.

Il consenso, secondo i principi generali richiamati dall'art. 23 del Codice (tale articolo è ricompreso in un capo dedicato ai soggetti privati, ma appunto perché per questi il consenso è una modalità normale di legittimazione, laddove per gli enti pubblici è un'eccezione), è validamente prestato dall'interessato (o da altro soggetto legittimato) solo:
- se è espresso liberamente;
- se è espresso specificamente in riferimento ad un trattamento chiaramente individuato;
- se è stata data idonea informativa all'interessato.

5.9 TITOLARE DEL TRATTAMENTO

L'art. 28 del Codice definisce Titolare il soggetto – persona fisica, persona giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo – cui competono le decisioni in ordine:
- alle finalità del trattamento,
- alle modalità di trattamento,
- agli strumenti utilizzati per effettuare il trattamento,
- ai profili della sicurezza.

Il Titolare, previsto dall'art. 28 del Codice, è il soggetto che assurge di fatto a centro di imputazione giuridica delle scelte di fondo sulle finalità, modalità, strumenti, inerenti al trattamento dei dati; è colui nel cui oggettivo interesse il trattamento è effettuato e che stabilisce se effettuare il trattamento, determinandone gli scopi e come deve essere eseguito.

Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione o organismo, titolare del trattamento è l'entità nel suo complesso; ne segue che, nel nostro caso, titolare del trattamento è l'Istituto (non il suo organo legale rappresentante, cioè il Direttore Generale).

E' dunque all'Istituto, quale titolare del trattamento, e non alle sue singole articolazioni organizzative e di responsabilità, che spetta il compito di operare le scelte di fondo sulle finalità, modalità, strumenti, inerenti al trattamento dei dati.

Il Titolare, con l'ausilio del Referente aziendale per la privacy, provvede ad assolvere agli obblighi previsti dalla normativa nazionale e dalle disposizioni regionali in materia di riservatezza dei dati personali, ed in particolare:
- effettua la notificazione al Garante ai sensi dell'articolo 37 del Codice;
- effettua le comunicazioni al Garante ai sensi dell'art. 39 del Codice;
- nomina i responsabili del trattamento, impartendo loro le necessarie istruzioni per la corretta gestione e tutela dei dati personali, ivi compresa la salvaguardia della loro integrità e sicurezza, e verificando periodicamente l'attività svolta rispetto alle istruzioni impartite.

5.10 CONTITOLARITÀ DEL TRATTAMENTO

Per un dato trattamento può essere configurata una situazione di contitolarità. Essa deve essere ricondotta ad una comunanza nella possibilità di determinare finalità e modi del trattamento, derivante dalla compartecipazione finale agli interessi in vista dei quali il trattamento è predisposto.

E' una condizione che si trova spesso correlata a progetti di interesse regionale o interistituzionale (con l'Università degli studi di Firenze) o interaziendale (con l'Azienda sanitaria di Firenze, l'Azienda Ospedaliero-Universitaria Meyer, l'AOU Careggi) o di Area Vasta, ecc..

5.11 RESPONSABILI DEL TRATTAMENTO

Si tratta di soggetti, individuati dal Titolare, che hanno il compito di collaborare per l'applicazione, nelle realtà operative di rispettiva competenza, delle idonee misure per assicurare il diritto alla protezione dei dati personali.

La loro individuazione, facoltativa per l'art. 29 del Codice, è stata prevista come obbligatoria, per gli enti sanitari, da Regione Toscana (cfr. Delibera G.R.T. del 29 novembre 2004 Linee guida alle Aziende sanitarie per l'applicazione del D.Lgs. 196/2003).

L'Istituto individua quali responsabili del trattamento:

- il **Direttore Amministrativo** e il **Direttore Sanitario**, ciascuno per il settore di rispettiva competenza e per tutte quelle operazioni facenti espressamente capo alla Direzione Aziendale;
- i **Direttori di strutture organizzative complesse e delle strutture semplici afferenti alla Direzione Aziendale** o, in vacanza di incarico, secondo quanto previsto, in tema di sostituzioni, dal vigente Regolamento di Organizzazione e Funzionamento dell'Istituto;
- i **Responsabili dei Coordinamenti assistenziale, tecnico-sanitario e statistico delle aree del Comparto** o, in vacanza di incarico, i coordinatori facenti funzione individuati dalla Direzione Aziendale.

Possono inoltre essere individuati dal Titolare, quali responsabili, altri dirigenti o funzionari, in virtù delle particolarità organizzative e funzionali delle attività di competenza.

Nell'ambito di un progetto di sperimentazione, lo sperimentatore principale (P.I.) è individuato quale responsabile del trattamento.

Il responsabile del trattamento ha il compito di individuare, in relazione ai trattamenti di dati personali effettuati nelle strutture afferenti alla propria area di competenza ed in collaborazione con il Referente aziendale per la privacy, adeguate misure organizzative e gestionali dirette ad assicurare a tutti i soggetti interessati il diritto alla riservatezza ed alla protezione dei dati personali e dunque ad evitare trattamenti dei dati non consentiti nonché ad assicurare una puntuale gestione degli archivi cartacei ed una corretta archiviazione dei dati trattati con strumenti informatici.

Più in particolare, relativamente ai trattamenti di dati personali effettuati nelle strutture afferenti alla propria area di competenza, il responsabile del trattamento, anche avvalendosi, ove occorra, della consulenza del Referente aziendale per la privacy, deve:

- vigilare sull'osservanza delle istruzioni impartite dal Titolare (in particolare con il presente documento);
- identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza. I Responsabili del trattamento periodicamente devono comunicare al Referente aziendale per la privacy e aggiornare, in caso di modifica, attivazione o cessazione, l'elenco dei trattamenti effettuati nell'ambito della propria struttura e le relative misure di sicurezza adottate.
- definire per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o anomizzazione dei dati obsoleti, nel rispetto della normativa in materia di tenuta archivi;

- far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti, in particolare, comunicare preventivamente al Titolare, per il tramite del Referente aziendale per la privacy, l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice;
- segnalare al Titolare, per il tramite del Referente aziendale per la privacy, l'eventuale cessazione del trattamento (art. 16 codice);
- verificare che all'interessato o al soggetto presso il quale sono raccolti i dati personali sia data l'informativa di cui all'art. 13 del Codice, se necessario coordinandosi con il Referente aziendale per la privacy per la sua redazione e modalità di comunicazione;
- verificare che l'interessato o altro soggetto legittimato presti, quando previsto, il consenso al trattamento dei dati;
- individuare tra i propri collaboratori gli Incaricati del trattamento, nominandoli con atto scritto che deve contenere anche le istruzioni cui devono attenersi nell'ambito del trattamento consentito – integrative di quelle fornite dal Titolare, precisando compiti e mansioni;
- stabilire idonei profili di autorizzazione dei propri incaricati agli applicativi informatici, nel rispetto dei principi di necessità, pertinenza e non eccedenza;
- assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali (art. 19 codice Privacy);
- attenersi, per i dati relativi ad attività di studio e di ricerca (art. 100 codice Privacy), alla disciplina secondo la quale è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
- adempiere agli obblighi di sicurezza, quali:
    - adottare le misure minime di sicurezza espressamente previste dal Codice (vedi allegato n. 3 al presente documento).
    - adottare tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione e perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 codice Privacy);
    - comunicare tempestivamente al Titolare casi di accesso non autorizzato ai dati o di trattamento non consentito o non conforme alle finalità istituzionali.

La funzione di Responsabile del trattamento dei dati, per il suo carattere fiduciario, è attribuita personalmente e non è suscettibile di delega.

I responsabili possono designare dei sostituti in caso di loro assenza o impedimento.

Il Responsabile del trattamento si avvale dei propri collaboratori per stabilire continuativi rapporti di informazione e coordinamento con il Referente aziendale per la privacy.

Il Responsabile del trattamento è formalmente delegato ad individuare, per i trattamenti di competenza, e con il supporto del Referente aziendale per la privacy, i soggetti esterni legittimati a trattare i dati personali di cui l'Azienda è Titolare.

Ogni modifica di responsabilità delle strutture organizzative afferenti al Responsabile del Trattamento deve essere segnalata al Referente.

5.12 RESPONSABILI ESTERNI DEL TRATTAMENTO

Vi sono situazioni in cui l'Istituto, esternalizzando un servizio, si trova a dover consentire ad un collaboratore esterno (che può essere tanto un soggetto pubblico in rapporto convenzionale che, più frequentemente, un soggetto privato) di accedere ai dati personali necessari per espletarlo. Il problema è che in tal caso verrebbe ad attuarsi una "comunicazione" di dati personali, definita dall'art. 4 comma 1 l) del Codice, come il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Il Codice prevede specifici requisiti normativi per la comunicazione dei dati comuni come sensibili o giudiziari da parte di un soggetto pubblico ad altro soggetto, pubblico o privato. Per evitare che si rientri in una fattispecie di comunicazione di dati personali (operazione che si riferisce "a uno o più soggetti determinati diversi dall'interessato, (...) dal responsabile e dagli incaricati"), qualora un contratto preveda l'accesso a dati personali di terzi, si ricorre pertanto alla nomina del soggetto esterno quale responsabile (esterno) del trattamento (se persona fisica, con un ambito di autonomia tecnico-organizzativa limitato, anche incaricato esterno del trattamento). Con tale soluzione si evita appunto la fattispecie comunicazione dei dati, riportando in certo qual modo la trasmissione di informazioni all'interno dell'ambito di legittimazione del Titolare. Il Responsabile entra così sostanzialmente a far parte del sistema privacy del Titolare: tale configurazione del rapporto legittima il soggetto esterno ad utilizzare, per la parte di competenza, i dati in possesso e nella titolarità del Titolare, vincolandolo però ad utilizzarli per le sole finalità da questi perseguite. Al responsabile esterno è riservata una parziale autonomia riguardante la sola concreta disciplina del servizio ed alcune scelte tecnico-operative, ma non anche le principali decisioni sulle finalità e sulle modalità di utilizzazione dei dati.
Il responsabile esterno risponderà dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli art. 1218 e 1223 del Codice Civile. La soluzione del responsabile esterno è ovviamente applicabile anche alla esternalizzazione di servizi verso altri soggetti pubblici: Estar è stata appunto individuata quale responsabile esterno del trattamento in ordine alle funzioni trasferite relative a Tecnologie sanitarie e Servizi ICT.
In tutti i contratti/convenzioni che disciplinano rapporti con soggetti esterni cui si delegano attività di competenza aziendale che comportano trattamento di dati personali, deve essere inserita la seguente clausola con la quale il soggetto esterno viene qualificato Responsabile esterno del trattamento:

XXXXXX è individuato da ISPO, in relazione al trattamento di dati di cui al presente provvedimento, RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'art. 29 del D.Lgs. 196/2003. XXXXXX, nell'effettuare le operazioni e i compiti affidati, si impegna ad attenersi al rispetto delle vigenti disposizioni normative in materia di protezione dei dati personali; in particolare si impegna a:
- effettuare il trattamento dei dati in modo lecito e corretto, nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- assumere le misure necessarie per evitare rischi di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- non effettuare operazioni di comunicazione o diffusione dei dati trattati qualora non previste da norme di legge o di regolamento;
- limitare l'accesso ai dati all'espletamento delle proprie mansioni e delle attività trasferite;
- informare il Titolare in caso di incidente di sicurezza;
- fornire in ogni momento le informazioni richieste e segnalare ogni questione rilevante ai fini dell'applicazione della normativa in materia di protezione dei dati;
- nominare per iscritto gli incaricati del trattamento, fornendo loro le necessarie istruzioni.

Normalmente, qualora non vi siano indicazioni in contrario, sono aggiunte le seguenti clausole:
La presente nomina:
- non contempla attribuzioni di responsabilità relativamente all'esattezza, aggiornamento, completezza, non eccedenza dei dati trattati rispetto alle finalità del trattamento, che restano in capo al Titolare del trattamento;
- non contempla attribuzioni di responsabilità relativamente all'ottemperanza ad altri obblighi normativi quali prestazione dell'informativa e acquisizione del consenso dell'interessato, che restano, qualora previsti dalla normativa, in capo al Titolare del trattamento.

Inoltre, qualora le attività delegate rientrino tra quelle dei c.d. Amministratori di sistema deve essere aggiunta la seguente clausola:
- considerato che tra le attività esternalizzate con il presente provvedimento rientrano anche servizi propri dei c.d. Amministratori di sistema (di cui al provvedimento dell'Autorità Garante per la protezione dei dati personali Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008 e successive modifiche ed integrazioni), XXXXXX si impegna a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Qualora quanto sopra non sia previsto nel contratto/convenzione, l'Istituto dovrà provvedere alla nomina a Responsabile esterno del trattamento con atto separato.

5.13 INCARICATO DEL TRATTAMENTO

Gli incaricati sono, ai sensi dell'art. 30 del Codice, le persone fisiche autorizzate a compiere operazioni di trattamento dal responsabile o dal titolare.
Sono coloro che materialmente effettuano, attenendosi alle istruzioni impartite dal titolare e dal responsabile, le operazioni di trattamento di dati: nel contesto aziendale, dunque, con modalità ed abilitazioni diverse secondo le rispettive competenze, trattasi tanto di personale sanitario che tecnico o amministrativo.
La designazione degli incaricati deve essere effettuata dal Responsabile del Trattamento per iscritto ed individuare puntualmente l'ambito del trattamento consentito (si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale sia individuato, per iscritto, l'ambito del trattamento consentito ai suoi addetti). La designazione deve essere aggiornata in relazione al trasferimento presso altra struttura dell'Istituto o alla modifica delle attribuzioni/competenze che modifichino i trattamenti dei dati personali per i quali è autorizzato l'incarico.

Il personale dipendente di ISPO incaricato di trattamento dei dati è individuato tramite lo schema contenuto **nell'allegato n. 1** al presente documento mentre il personale non dipendente è individuato tramite lo schema contenuto **nell'allegato n. 2.**
Il presente documento e i successivi documenti di settore costituiscono le istruzioni del Titolare del trattamento al personale ISPO sia sanitario che tecnico amministrativo.
I responsabili del trattamento dovranno, a loro volta, qualora ritenuto opportuno o necessario, predisporre indicazioni scritte agli incaricati di propria pertinenza – distinti per categorie – integrative di quelle fornite dal Titolare sull'ambito di trattamento consentito, precisando compiti e mansioni.
L'ambito dei trattamenti consentiti ai singoli incaricati e gestiti con supporti informatici e/o cartacei, necessari all'espletamento delle attività istituzionali, deve esser verificato ed aggiornato periodicamente dal Responsabile del Trattamento, con cadenza almeno annuale.
Gli incaricati possono aver accesso esclusivamente ai dati personali la cui conoscenza sia strettamente necessaria o indispensabile per l'espletamento delle attività cui sono preposti.
In ambito sanitario, specifica l'art. 85 comma 4 del Codice:
"L'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività (...) secondo il principio dell'indispensabilità dei dati di volta in volta trattati".
Le designazioni sono estese, con analoghi criteri e modalità, anche ai non dipendenti, e più in particolare a quei soggetti che funzionalmente svolgono operazioni di trattamento su dati di cui l'Istituto ha la titolarità, quali i soggetti con incarico libero professionale o altro personale non strutturato. Ciò vale ovviamente anche, ove non previsto da specifiche Convenzioni di ISPO con strutture pubbliche o private, per dottorandi di ricerca, borsisti, nonché volontari, tirocinanti o laureandi che accedano ai pazienti per acquisire informazioni necessarie per la tesi (si sottolinea che la somministrazione di un questionario prevede anche la comunicazione agli interessati di una idonea informativa sul trattamento dei dati). Insomma, tutti i soggetti che a qualsiasi titolo e per qualsivoglia legittima ragione accedono, a seguito di autorizzazione dell'Istituto, alle strutture assistenziali (così trattando dati personali di cui l'Istituto è titolare), devono essere individuati, con modalità ed abilitazioni diverse secondo le rispettive competenze ed i diversi contesti operativi, quali incaricati del trattamento dei dati ai sensi dell'art. 30 del Codice (si veda lo schema allegato n. 2 al presente documento). Restano esclusi da tale obbligo i soggetti di per sé legittimati, ad es. agenti NAS che effettuano un'ispezione. Ai sensi dell'art. 83 comma 2 i del Codice, anche gli incaricati del trattamento che non sono tenuti per legge al segreto professionale, sono sottoposti a regole di condotta analoghe al segreto professionale.

5.14 FORMAZIONE DEGLI INCARICATI

L'Istituto, ai sensi del punto 19.6 dell'allegato B al Codice, prevede interventi formativi degli incaricati del trattamento, per renderli edotti dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano, nonché dei rischi che incombono sui dati e delle misure disponibili per prevenire eventi dannosi. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

5.15 REFERENTE AZIENDALE PER LA PRIVACY

Il Referente aziendale per la privacy viene nominato con atto del Direttore Generale, su proposta del Direttore Amministrativo e svolge i seguenti compiti:

- garantisce il supporto alla Direzione Aziendale nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia, segnatamente in tema di notificazione al Garante ex art. 37 del Codice e comunicazioni al Garante ex artt. 39 e 41 del Codice;
- vigila sull'osservanza delle istruzioni contenute nel presente documento;
- tiene ed aggiorna un censimento dei trattamenti effettuati in Istituto sulla base delle comunicazioni effettuate dai responsabili del trattamento;
- tiene e aggiorna l'elenco dei responsabili del trattamento in ambito aziendale;
- tiene ed aggiorna l'elenco degli archivi cartacei e/o magnetici contenenti dati personali custoditi a livello aziendale, sulla base delle informazioni inviategli dai responsabili delle strutture competenti;
- propone, svolge e/o coordina l'attività di formazione in tema di normativa sulla riservatezza dei dati, assicurando la promozione della cultura della privacy a livello aziendale;
- gestisce i riscontri alle istanze degli interessati ex art. 7 del Codice, e si attiva per comporre le controversie sui dati personali;
- fornisce la necessaria consulenza in ordine alle problematiche in tema di riservatezza, in particolare collaborando con i responsabili del trattamento;
- propone l'adeguamento dei percorsi e delle procedure aziendali per quanto attiene l'aspetto della riservatezza dei dati;
- si occupa dei conflitti tra diritto alla riservatezza dei dati e dovere di garantire la trasparenza dell'attività amministrativa.

5.16 INCARICATO DEL TRATTAMENTO "AMMINISTRATORE DI SISTEMA"

Con il Provvedimento Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (del 27 novembre 2008) e successive modifiche ed integrazioni (provvedimenti del 27 novembre 2008 e 25 giugno 2009), l'Autorità Garante ha prescritto l'adozione di specifiche misure e cautele in riferimento alle mansioni svolte dagli amministratori di sistema e dai soggetti (di profilo anche non strettamente tecnico-informatico) ad essi assimilabili.

La nozione di amministratore di sistema, funzionale all'adempimento, è estremamente ampia e ricomprende anche attività non di esclusiva competenza di tecnici informatici (ad es. la gestione dei sistemi di autenticazione e di autorizzazione). Nell'ambito del Provvedimento del Garante, l'amministratore di sistema è assunto quale figura professionale dedicata in senso lato alla gestione e alla manutenzione di impianti di elaborazione (compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza) con cui vengano effettuati trattamenti di dati personali, e nella misura in cui consentano di intervenire sui dati personali. Rientrano dunque in questa accezione ampia una serie di figure chiamate a svolgere funzioni che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e a dati personali (anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo), e nella misura in

cui sono, nelle loro consuete attività tecniche, "responsabili" di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:
- gestione dei sistemi di autenticazione e di autorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- salvataggio dei dati (backup/recovery);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- manutenzione hardware.

Possono dunque qualificarsi quale Amministratori di sistema i seguenti soggetti:
- amministratori di sistemi di autenticazione e di autorizzazione;
- amministratori di server;
- amministratori di apparati rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es. per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di elaborazione e sui sistemi software.

In riferimento a tale ampia definizione di amministratore di sistema, il Provvedimento del Garante ha prescritto:
- una designazione nominativa degli incaricati del trattamento che svolgano tali funzioni;
- una puntuale ed analitica indicazione dei compiti loro assegnati;
- la redazione di un documento interno che riporti gli estremi identificativi delle persone fisiche amministratori di sistema (nome, cognome, area organizzativa di appartenenza), con l'elenco delle funzioni ad essi attribuite;
- l'adozione di accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte dell' Istituto quale Titolare del trattamento.

Qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale di dipendenti, l'Istituto è tenuto a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito della propria organizzazione.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing, il fornitore del servizio – da individuarsi, in accordo con le prescrizioni di carattere generale, quale Responsabile esterno del trattamento – dovrà impegnarsi a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

5.17 ATTIVITÀ NORMATIVA DELL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali è un organo collegiale, costituito da quattro componenti scelti tra esperti di riconosciuta competenza nelle materie del diritto o dell'informatica, che ha i seguenti compiti (elencati all'art. 154 comma 1 del Codice):
- controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile;
- esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati;

- prescrivere, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;
- vietare, anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco;
- promuovere la sottoscrizione di codici deontologici;
- esprimere pareri, nei casi previsti;
- curare la conoscenza, tra il pubblico, della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonchè delle misure di sicurezza dei dati.

Rispetto ad altre autorità indipendenti, il Garante per la protezione dei dati personali si caratterizza per il rilievo che assumono i seguenti ordini di funzioni:
- funzioni paragiurisdizionali, come organo alternativo alla giustizia ordinaria che ha il compito di pronunciarsi con decisione motivata sui ricorsi presentatigli (art. 145 del Codice);
- poteri di indirizzo e promozione (art. 154 del Codice);
- poteri di accertamento e di ispezione (artt. 157 sgg. del Codice);
- poteri sanzionatori (art. 161 sgg. del Codice).

Di fatto al Garante ed in maggior misura rispetto ad altre autorità di garanzia, è riconosciuta una vera e propria funzione di legal implementation, nel senso che, qualora individui regole e prescrizioni relative ad un determinato ambito di trattamento, queste non si qualificano come meri suggerimenti, ma come vere e proprie norme, vincolanti e cogenti, alle quali il Titolare deve adeguarsi nei termini previsti, pena l'applicazione di sanzioni.

Oltre che di tali poteri di carattere sostanzialmente normativo, il Garante dispone anche di poteri provvedimentali. Unico tra le autorità indipendenti, dispone cioè del potere di assicurare ai privati, oltre ad una tutela di carattere amministrativo (attraverso la proposizione di segnalazioni e reclami), una tutela di fatto alternativa a quella giurisdizionale. L'interessato che lamenti una lesione dei propri diritti di protezione dei dati personali può infatti rivolgersi al giudice ordinario o al Garante (se si rivolge al giudice, non può però rivolgersi al Garante, laddove se si rivolge al Garante può comunque poi sempre adire le vie giudiziarie, nel rispetto dell'art. 23 comma 1 Cost., per il quale "Tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi").

5.18 OBBLIGHI DI NOTIFICAZIONE AL GARANTE

Ai sensi dell'art. 37 del Codice, corre l'obbligo di notificare al Garante il trattamento di dati personali che riguardi determinati dati e contesti, specificati all'art. 37 comma 1 del Codice, tra i quali:
- dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Il Garante può individuare, con proprio provvedimento, altri trattamenti, rispetto a quelli individuati dall'art. 37 comma 1 del Codice, suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali e dunque sottoposti all'obbligo di notificazione. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento già notificato o al mutamento di taluno degli elementi da indicare nella notificazione medesima; è inoltre richiesta, evidentemente, nel caso di nuovo trattamento ricompreso in una tipologia di trattamento non precedentemente notificata.

La procedura di notificazione è seguita dal Referente aziendale per la privacy. E' fatto obbligo a ciascun responsabile del trattamento di fornire al Referente aziendale per la privacy tutti gli elementi informativi necessari per effettuare la notificazione di cui sopra quale presupposto di legittimità del trattamento che si intende attivare.

5.19 OBBLIGHI DI COMUNICAZIONE AL GARANTE

Ai sensi dell'art. 39 del Codice, il Titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:

- 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 (qualora eventualmente non sia opportuno o possibile attivare la soluzione del c.d. responsabile esterno del trattamento); - trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, e di cui all'articolo 110, comma 1, primo periodo del Codice.

E' fatto obbligo a ciascun responsabile (interno o esterno) del trattamento di fornire al Referente aziendale per la privacy tutti gli elementi informativi necessari per effettuare la comunicazione di cui sopra, quale presupposto di legittimità del trattamento che si intende attivare. I trattamenti oggetto di comunicazione possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione, salvo diversa determinazione anche successiva del Garante.

Il Provvedimento Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario del 16 luglio 2009 ha previsto che siano oggetto di comunicazione al Garante i trattamenti di dati personali effettuati attraverso il fascicolo sanitario elettronico (insieme logico di informazioni e documenti sanitari volto a documentare la storia clinica di un individuo condiviso da più titolari del trattamento). A tale obbligo può adempiere anche l'ente capofila (nel ns. caso ha adempiuto la Regione Toscana).

5.20 MISURE DI SICUREZZA MINIME E IDONEE

Nel quadro dei più generali obblighi di sicurezza, i titolari del trattamento sono tenuti ad adottare alcune misure minime, indicate agli artt. 33-35 del Codice e dettagliate nell'Allegato B - Disciplinare tecnico in materia di misure minime di sicurezza al Codice, diversificate per i trattamenti effettuati senza o con l'ausilio di strumenti elettronici (vedi **allegato n. 3** al presente documento). L'adozione delle misure minime di sicurezza, intese come il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31 del D.Lgs. 196/2003, ossia "*i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*", è condizione di legittimità del relativo trattamento: ciò significa che un trattamento eseguito senza che siano adottate le relative misure minime di sicurezza è illegittimo (sono anche previste sanzioni di carattere amministrativo e penale). Le misure minime sono precisate in un Disciplinare Tecnico allegato B al Codice, "aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore" (art. 36 del Codice).

5.21 SANZIONI

Il Titolo III del Codice elenca le sanzioni di tipo amministrativo e di tipo penale che hanno origine dall'inosservanza delle disposizioni in materia di protezione dei dati personali prescritte per legge. A titolo esemplificativo, tra quelle che danno vita a illecito amministrativo, ci sono l'omessa o inidonea informativa all'interessato (pena pecuniaria da seimila euro a trentaseimila euro), l'omessa o incompleta notificazione al garante (pena pecuniaria da ventimila euro a centoventimila euro) l'omessa informazione o esibizione al Garante (pena pecuniaria da diecimila euro a sessantamila euro) mentre, tra gli illeciti penali, sono da annoverare il trattamento illecito di dati (reclusione da sei a diciotto mesi), la falsità nelle dichiarazioni e notificazioni al Garante (reclusione da sei mesi a tre anni), misure di sicurezza (arresto sino a due anni), l'inosservanza di provvedimenti del Garante (reclusione da tre mesi a due anni).

6. DEFINIZIONI

Dati personali: qualunque informazione relativa ad un soggetto - persona fisica, persona giuridica, ente od associazione - identificato o identificabile (anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale).

Dati anonimi: i dati che, in origine o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile.

Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati idonei a rivelare lo stato di salute: informazioni tali da svelare, anche indirettamente ("idonei a ...") uno stato patologico o comunque almeno uno stato di normalità compromessa.

Dati giudiziari: i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato.
Dati genetici: i dati che, indipendentemente dalla tipologia, identificano le caratteristiche del patrimonio genetico di un individuo trasmissibili nell'ambito di un gruppo di persone legate da vincoli di parentela.
Trattamento: qualunque operazione o complesso di operazioni effettuato sui dati personali (raccolta, registrazione, organizzazione, conservazione; consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco comunicazione, diffusione, cancellazione, distruzione di dati). Rientrano nella nozione di trattamento anche le operazioni effettuate senza l'ausilio di strumenti elettronici, nonché quelle relative ad informazioni non organizzate in banche dati.
Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati (diversi dall'interessato, dal responsabile e dagli incaricati), in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Trasferimento: ogni spostamento anche temporaneo di informazioni, tanto all'interno che all'esterno dell'ambito di titolarità del trattamento.
Titolare: il soggetto - persona fisica, persona giuridica, pubblica amministrazione o 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. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso.
Responsabile: il soggetto - persona fisica, persona giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo - preposto dal Titolare al trattamento di dati personali.
Incaricato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal responsabile, in pratica chi materialmente effettua le operazioni di trattamento di dati.
Interessato: il soggetto (persona fisica, persona giuridica, ente o associazione) cui si riferiscono i dati personali.
Amministratore di sistema: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Garante per la Protezione dei dati personali: organo collegiale che ha, tra l'altro, il compito di:
- controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile;
- esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati;
- prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;
- vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco;
- promuovere la sottoscrizione di codici deontologici;

- esprimere pareri nei casi previsti.

Gruppo di lavoro ex articolo 29 direttiva 95/46/CE: istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle Autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.

Allegato n. 1 A0070

ATTO DI DESIGNAZIONE A

INCARICATO DEL TRATTAMENTO DEI DATI

Il Sig/ La Sig.ra _____ dipendente di ISPO presso la Struttura Organizzativa Semplice/Complessa _____ con la qualifica di _____ è designato/a quale incaricato del trattamento ai sensi dell'art. 30 del Codice in materia di protezione dei dati personali (D.lgs. 30 giugno 2003 n. 196), in relazione alle attività connesse allo svolgimento della propria mansione.

L'incaricato ha il dovere di effettuare il trattamento dei dati in modo lecito e corretto e nel rispetto delle norme di legge, ed in particolare ha il dovere di:

- rispettare le istruzioni impartite dal Titolare e dal responsabile del trattamento;
- rispettare le misure di sicurezza predisposte dal Titolare;
- non effettuare operazioni di comunicazione o diffusione dei dati trattati qualora non previste da norme di legge o di regolamento;
- limitare l'accesso ai dati indispensabili all'espletamento delle proprie mansioni;
- verificare, in caso di interruzione, anche temporanea, del lavoro, che i dati trattati non siano accessibili a terzi non autorizzati.

Si ricorda che, ai sensi dell'art. 83 comma 2 i) del D.lgs. 30 giugno 2003 n. 196, anche gli incaricati del trattamento che non sono tenuti per legge al segreto professionale, sono sottoposti a regole di condotta analoghe al segreto professionale.

Firenze, addì .....

Il Responsabile del trattamento .....

Firma per presa visione

_____

Allegato n. 2 A0070

ATTO DI DESIGNAZIONE A

INCARICATO DEL TRATTAMENTO DEI DATI

Il Sig/ La Sig.ra _____ è designato/a quale incaricato del trattamento ai sensi dell'art. 30 del Codice in materia di protezione dei dati personali (D.lgs. 30 giugno 2003 n. 196), in relazione alle attività necessarie per _____

_____.

L'incaricato ha il dovere di effettuare il trattamento dei dati in modo lecito e corretto e nel rispetto delle norme di legge, ed in particolare ha il dovere di:

- rispettare le istruzioni impartite dal Titolare e dal responsabile del trattamento;
- rispettare le misure di sicurezza predisposte dal Titolare;
- non effettuare operazioni di comunicazione o diffusione dei dati trattati qualora non previste da norme di legge o di regolamento;
- limitare l'accesso ai dati indispensabili all'espletamento delle proprie mansioni;
- verificare, in caso di interruzione, anche temporanea, del lavoro, che i dati trattati non siano accessibili a terzi non autorizzati.

Si ricorda che, ai sensi dell'art. 83 comma 2 i) del D.lgs. 30 giugno 2003 n. 196, anche gli incaricati del trattamento che non sono tenuti per legge al segreto professionale, sono sottoposti a regole di condotta analoghe al segreto professionale.

Firenze, addì .....

Il Responsabile del trattamento .....

Firma per presa visione

_____

ALLEGATO N. 5 AUTO

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Codice in materia di protezione dei dati personali
B. Disciplinare tecnico in materia di misure minime di sicurezza
(Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari

l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza
19. [soppresso] (1)

19.1. [soppresso](1)
19.2. [soppresso](1)
19.3. [soppresso](1)
19.4. [soppresso](1)
19.5. [soppresso](1)
19.6. [soppresso](1)
19.7. [soppresso](1)
19.8. [soppresso](1)

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il 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 non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono 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 dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. [soppresso] (1)

Trattamenti senza l'ausilio di strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

(1) Paragrafi soppressi dall'art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

Per completezza, si riporta di seguito il testo dei paragrafi soppressi.

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

ALLEGATI

- Codice in materia di protezione dei dati personali
- Allegato A.1. Codice di deontologia - Trattamento dei dati personali nell'esercizio dell'attività giornalistica
- Allegato A.2. Codici di deontologia - Trattamento dei dati personali per scopi storici
- Allegato A.3. Codice di deontologia - Trattamento dei dati personali a scopi statistici in ambito Sistan
- Allegato A.4. Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici
- Allegato A.5. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti
- Allegato A.6. Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive
- Allegato C. Trattamenti non occasionali effettuatio in ambito giudiziario o per fini di polizia
- Tavola di corrispondenza dei riferimenti previgenti al codice in materia di protezione dei dati personali