Servizio Sanitario della Puglia
Azienda Sanitaria Locale Lecce
Sede Legale e Direzione Generale

DELIBERAZIONE DEL DIRETTORE GENERALE

DELIBERAZIONE NUMERO	1185	DEL	11 LUG. 2013

OGGETTO:	Regolamento per la Protezione dei Dati Personali - Recepimento - Individuazione Responsabile Aziendale – Responsabili – Ufficio Privacy

L'anno 2013, il giorno Venerdì del mese di luglio in Lecce, nella Sede della Azienda , in via Miglietta n.5

STRUTTURA (Codice)	CENTRO DI COSTO (Codice)

STRUTTURA (Descrizione)	CENTRO DI COSTO (Descrizione)

IL DIRETTORE GENERALE

- Visto il D.Lgs. 30/12/1992 n.502 e successive modifiche ed integrazioni;
- Vista la Legge Regionale 28/12/1994, n.36;
- Vista la Legge Regionale 30/12/1994, n.38;
- Vista la Legge Regionale 03/08/2006 n. 25;
- Vista la Legge Regionale 28/12/2006 n. 39;
- Vista la L.R. 25.2.2010, n.4;
- Vista la Deliberazione della Giunta Regionale n.2504 del 15.11.2011;
- Coadiuvato dal Direttore Amministrativo e dal Direttore Sanitario;

Il dottore Cappelluti Tasti relaziona in merito:

Premesso che:

- La normativa nazionale – in particolare il cosiddetto Codice Privacy e le regolamentazioni da esso scaturenti - fissa rilevanti vincoli ed elementi prescrittivi in merito al trattamento di dati personali stabilendo al contempo ulteriori obblighi in presenza di dati sensibili
- L'Azienda Sanitaria – per suo stesso compito istituzionale – tratta – nella maggioranza dei casi - dati relativi alla salute degli assistibili (sensibili)
- La vastità e complessità dell'organizzazione aziendale, le diverse "linee di produzione" ed i molteplici punti di erogazione del servizio sono fattori che rendono l'applicazione delle prescrizioni normative e l'implementazione delle "misure minime di sicurezza" possibili solo in presenza di una forte volontà aziendale unita ad una visione strategica degli interventi da effettuarsi
- La Regione Puglia con Legge Regionale n. 4 del 2010 ha indicato come necessaria l'istituzione di una funzione dedicata alla gestione delle problematiche relative al trattamento dei dati personali e sensibili al fine di garantire l'attuazione di quanto contenuto nel D.lgs. 196/2003 e nel Regolamento Regionale n. 5/2006
- Con DDG 3978 del 31.12.2010 e DCS 2380 del 16.11.2011 si è proceduto a definire l'assetto organizzativo della Dirigenza dei ruoli Professionale, Tecnico ed Amministrativo
- Con DDG 156 del 26.01.2012 si è conferito l'incarico di Alta Professionalità per la struttura in staff alla Direzione Generale "Amministrazione Digitale, Sicurezza e Privacy" al dottore Antonio Cappelluti Tasti che – così come da contratto individuale di lavoro – ha il compito – rispetto all'ambito Privacy - di:
  - Implementare le Misure Minime di Sicurezza
  - Omogeneizzare ed Uniformare la Modulistica
  - Pianificare, Coordinare ed Erogare piani e Contenuti Formativi
  - Predisporre Atti e Documenti a Contenuto Privacy
  - Definire e Monitorare le Misure Privacy per i Prestatori di Servizi e/o dei Provider Esterni
  - Definire il "decalogo operandi" Aziendale
- Uno dei principali ambiti di intervento è legato alla redazione degli atti e documenti aziendali in presenza della necessità di bilanciamento delle prescrizioni amministrative, legali, privacy e di trasparenza dell'operato della P.A.
- Tale esigenza assume fondamentale importanza rispetto alla sempre più differenziata tipologia di documentazione destinata alla diffusione "erga omnes" ovvero ad un accesso facilitato attraverso le funzionalità proprie del Portale Internet Aziendale
- Lo stesso Garante Privacy ha posto grande attenzione rispetto ai – non evidenti ai più – potenziali rischi e dettato – di conseguenza - linee guida in ordine alla pubblicazione dei contenuti e della documentazione della P.A. su Internet

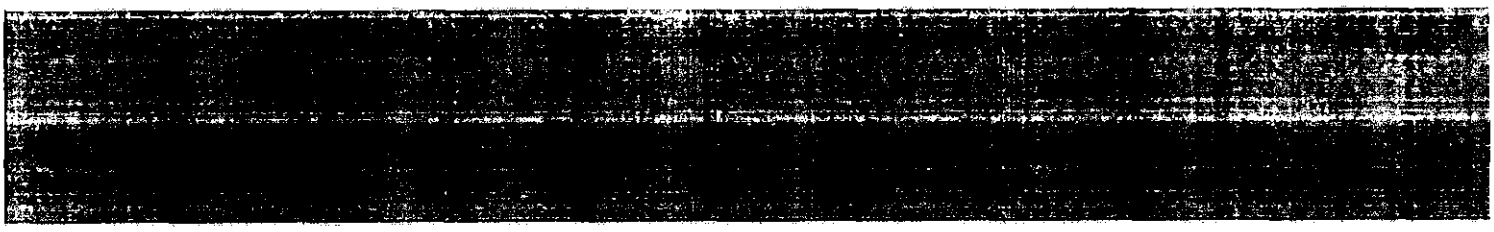
- Il processo di messa in disponibilità di detta documentazione è destinato – vedi Codice dell'Amministrazione Digitale, Decreto "Semplifica Italia", Agenda Digitale Italiana, etc. – a crescere in numero e tipologia

Atteso che:

- La definizione funzionale della struttura "Amministrazione Digitale, Sicurezza e Privacy" è frutto della valutazione dello stretto legame esistente tra gli elementi connessi all'implementazione del "digitale" all'interno della Pubblica Amministrazione, agli aspetti di "sicurezza logica" dei sistemi informatici ed informativi – visti quale infrastruttura di riferimento – e la tutela dei dati personali – in ambito privacy
- Di fatto la struttura "Amministrazione Digitale, Sicurezza e Privacy" ha ulteriori compiti quali:
  - Implementazione degli elementi di Digitalizzazione dell'Attività Amministrativa
  - Definizione dei contenuti tecnici ed organizzativi per la tenuta dei Rapporti tra Pubbliche Amministrazioni e Rapporti con Cittadini ed imprese
  - Accesso, Fruibilità e Trasparenza delle informazioni e dei Servizi in Rete
  - Implementazione delle Politiche di Identity management
- Il processo di pubblicazione della documentazione di natura non puramente informativa (deliberazioni, determinazioni, gare, concorsi, etc.) sul portale aziendale – pur se non formalmente regolamentato – è già assoggettato ad un consolidato processo di revisione privacy effettuato da collaboratori specificamente formati con l'informale supervisione del responsabile della struttura "Amministrazione Digitale, Sicurezza e Privacy"

Propone di:

- Approvare l'allegato "Regolamento per la Protezione dei Dati Personali - D.Lgs. 196/03 - Codice Privacy"
- Procedere all'individuazione formale del Responsabile Aziendale Privacy, conferendo allo stesso le funzioni previste nel RegolamentoProcedere all'individuazione formale dei Responsabili Privacy nel rispetto di quanto previsto nel Regolamento
- Procedere all'istituzione formale dell'"Ufficio Privacy", assegnando allo stesso i compiti previsti nel Regolamento
- Far confluire – per quanto già sopra indicato – l'Ufficio Privacy all'interno della struttura Amministrazione Digitale, Sicurezza e Privacy
- Individuare il Portale Intranet Aziendale – attraverso le funzionalità di gestione dei contenuti informativi e documentali - quale strumento di elezione per la messa in disponibilità e diffusione delle iniziative e dei contenuti privacy all'interno della Azienda
- Attivare – per l'intera Azienda Sanitaria - il processo di rilevazione dei trattamenti effettuati con la contestuale individuazione formale degli incaricati e la conseguente implementazione del registro elettronico
- Assoggettare al processo di revisione privacy – in forma propedeutica alla Pubblicazione - tutti gli atti e documenti aziendali destinati alla diffusione "erga omnes" ovvero ad un accesso facilitato attraverso il Portale Internet Aziendale
- Attivare il processo di revisione ed omogeneizzazione delle misure privacy sino ad ora intraprese con particolare riguardo a modulistica, gestione strumentazione elettronica, video sorveglianza



ASL LECCE

Regolamento per la Protezione dei Dati Personali

D.Lgs. 196/03 Codice Privacy

Cappelluti Tasti - TcT

Revisione 0.9 -

Indice

Scopo del Documento

Il Regolamento Aziendale sulla Privacy è uno degli strumenti di applicazione del D. Lgs. 30 giugno 2003 n. 196 - Codice Privacy - con successive modificazioni ed integrazioni, relativo alla tutela della riservatezza dei dati personali.

Come tale non rappresenta un'ulteriore aggravio normativo né tantomeno una limitazione dell'autonomia gestionale dei singoli responsabili bensì un complemento strumentale alla applicazione sostanziale delle prescrizioni privacy in tutti gli ambiti di trattamento di dati personali a livello aziendale.

Il regolamento assume una valenza maggiore di quella classica in quanto detta linee di comportamento all'interno della Azienda Sanitaria che – per fini istituzionali – tratta dati personali relativi alla salute degli assistiti. Per questi trattamenti il Codice Privacy contempla specifici vincoli e misure di sicurezza particolarmente stringenti.

Il documento è destinato – di conseguenza – a costituire nel contempo base informativa comune e strumento di regolamentazione con impatto sia sull'organizzazione del lavoro che sul modus operandi per ognuna della attività oggetto di trattamento di dati personali.

Come meglio esplicitato di seguito risulta fondamentale il ruolo e l'attività del RAP - Responsabile Aziendale Privacy – e dell'Ufficio Privacy destinati a svolgere rispettivamente la funzione di coordinatore e di primo attuatore delle iniziate privacy (non ultima la formazione degli operatori) e di consulenza in materia di applicazione delle prescrizioni privacy all'interno delle strutture aziendali.

Le prescrizioni contenute nel presente Regolamento devono intendersi come impartite dal Titolare del trattamento ai sensi dell'art. 28 del D.Lgs. n. 196/2003.

Normativa di Riferimento

Normativa Nazionale

Legge n. 241 del 7 agosto 1990 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi

Decreto Legislativo n. 196 del 30 giugno 2003 e ss.mm.ii. - Codice in Materia di Dati Personali

Decreto Legislativo 196/2003 - Allegato A.4. Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici

Decreto Legislativo 196/2003 - Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza

Decreto Legge 9 novembre 2004, n. 266 - Proroga o differimento di termini previsti da disposizioni legislative

Legge 27 luglio 2004, n. 188 - Conversione in legge, con modificazioni, del D.L. 24 giugno 2004, n. 158, concernente [...], nonché di protezione dei dati personali

Legge 4 marzo 2009, n. 15 - Delega al Governo finalizzata all'ottimizzazione della produttività del lavoro pubblico e alla efficienza e trasparenza delle pubbliche amministrazioni nonché disposizioni integrative delle funzioni attribuite al Consiglio nazionale dell'economia e del lavoro e alla Corte dei conti

Decreto legge 13 maggio 2011, n. 70 convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106

Decreto legge 9 febbraio 2012, n. 5 - Recante disposizioni urgenti in materia di semplificazione e di sviluppo, convertito con modificazioni, dalla Legge 4 aprile 2012, n. 35

Decreto legislativo 28 maggio 2012 , n. 69 - Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche,

e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori

Normativa Regionale

Regolamento Regionale n. 5 del 2006 "Regolamento per il Trattamento dei Dati Sensibili e Giudiziari ai sensi degli artt. 20 e 21 del Decreto Legislativo 196/03"
Legge Regionale n. 4 del 2010 "Norme urgenti in materia di sanità e servizi Sociali"
D.G.R. n° 2339 del 3 novembre 2010 "Gruppo di lavoro per la Privacy. Istituzione."

Normativa Aziendale

D.C.S. n. 861 del 27 marzo 2007 "Decreto Legislativo n° 196 30.6.2003 – Codice in materia di protezione dei dati personali – Approvazione Documento Programmatico di ricognizione, riorganizzazione ed adeguamento delle politiche di sicurezza nelle operazioni di trattamento di dati personali e sensibili nelle strutture della ASL "
D.D.G. 3651 del 7 dicembre 2010 "Massimario di Scarto – Modalità e termini temporali di archiviazione dei documenti e atti della ASL Lecce"
D.D.G. 348 del 11 febbraio 2011 "Delibera n. 3651 del 7/12/2010: Massimario di Scarto – Modalità e termini temporali di archiviazione dei documenti e atti della ASL Lecce: integrazione"

Definizioni

Ai fini del presente regolamento si applicano le definizioni contenute nell'art. 4 del D.Lgs. 196/2003 come di seguito specificate:

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 di dati

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

Dati Identificativi

i dati personali che permettono l'identificazione diretta dell'interessato

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 Giudiziari

i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, 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 articoli 60 e 61 del codice di procedura penale

Titolare

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

Responsabile

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

Incaricati

le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Interessato

la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali

Comunicazione

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

Diffusione

il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

Dato Anonimo

il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

Blocco

la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento

Banca di Dati

qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti

Garante

l'autorità di cui all'articolo 153, istituita dalla Legge 31 dicembre 1996, n. 675

Comunicazione Elettronica

ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile

Reti di Comunicazione Elettronica

i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato

Dati Relativi al Traffico

qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione

Dati Relativi all'Ubicazione

ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico

Posta Elettronica

messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza

Misure Minime

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'articolo 31 del Codice Privacy

Strumenti Elettronici

gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento

Autenticazione Informatica

l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità

Credenziali di Autenticazione

i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica

Parola Chiave

componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

Profilo di Autorizzazione

l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti

Sistema di Autorizzazione

l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente

Scopi Statistici

le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici

Scopi Scientifici

le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore

Ambito di Applicazione

Soggetti Autorizzati

Nel rispetto di quanto previsto dal Codice Privacy il trattamento di dati personali è ammesso solo da parte dei soggetti di seguito indicati:

Titolare
Responsabili del trattamento dei dati
Incaricati

L'Azienda non consente il trattamento dei dati da parte di personale non autorizzato.

Titolare

Il Titolare è l'Azienda Sanitaria Locale di Lecce. Il Direttore Generale della ASL, in qualità di rappresentante legale, procede agli obblighi previsti dal Codice Privacy (in particolare art .1 4 e art. 39) e dai regolamenti attuativi.

Il Titolare designa - quali Responsabili del trattamento dei dati - i Direttori delle Unità Operative Complesse aziendali ed i Responsabili delle Unità Operative in Staff o alle dirette dipendenze delle Direzioni Generale, Sanitaria ed Amministrativa, nonché il Responsabile della Segreteria della stessa Direzione Generale, il Direttore Sanitario ed il Direttore Amministrativo limitatamente alle relative strutture di Segreteria.

La designazione avviene con atto formale notificato con modalità che ne assicurino e ne provino in forma documentata l'avvenuta conoscenza.

Il Titolare individua, con modalità analoghe, il Responsabile Aziendale Privacy e il/gli Amministratori di Sistema.

Responsabile Aziendale - RAP

Il Responsabile Aziendale Privacy, formalmente individuato dal Titolare, assolve i seguenti principali compiti:

Coadiuva il Titolare nello svolgimento degli adempimenti di cui al precedente paragrafo
Assiste il Titolare nei rapporti con il Garante e coadiuva il Titolare ed i Responsabili del trattamento nei rapporti con altri soggetti pubblici o privati
Coordina le iniziative privacy a valenza aziendale
Predispone con la collaborazione, in particolare del/degli Amministratori di Sistema e del Responsabile dei Sistemi Informativi, oltre che dei responsabili individuati il documento programmatico semplificato sulla sicurezza dei dati - DPSS - e ne cura costantemente l'aggiornamento
Rende disponibili ai responsabili del trattamento dei dati personali ed agli incaricati la normativa, la regolamentazione nonché tutta la specifica documentazione privacy prodotta aziendalmente
Vigila sull'osservanza del presente regolamento ed, in generale, delle prescrizioni privacy, riportando al Titolare situazioni irrisolte ed eventuali patologie di sistema
Fornisce consulenza ai responsabili su specifiche problematiche privacy
Implementa la basi di dati relative ai trattamenti aziendali dei dati personali e dei responsabili

dei trattamenti aziendali ed esterni (a tal fine l'Area Gestione del Personale informa tempestivamente il RAP in presenza di atti di attribuzione di responsabilità di strutture organizzative ed ogni eventuale successiva variazione intervenuta)

Implementa le FAQ aziendali da utilizzarsi da parte degli incaricati da adoperarsi sia per attuare comportamenti a norma nell'espletamento delle attività istituzionali sia per fornire informazioni all'utenza relative all'applicazione della normativa privacy

Cura la produzione della modulistica e della cartellonistica

Propone e cura gli interventi di formazione privacy all'interno dei piani di formazione aziendali

Ufficio Privacy

L'Ufficio Privacy - direttamente coordinato dal RAP - si configura come supporto operativo e primo attuatore delle iniziate privacy aziendali. In particolare è destinato a fornire consulenza ai singoli operatori per la corretta applicazione delle prescrizioni privacy all'interno delle strutture aziendali. In particolare:

- ❑ Aggiorna i registri dei trattamenti, dei responsabili e degli incaricati, coadiuvando il RAP nella redazione e nella tenuta del DPSS.
- ❑ Si occupa - assieme al RAP - della predisposizione dei contenuti e dell'erogazione degli interventi formativi nello specifico settore.
- ❑ Cura la verifica ultima della conformità privacy di tutta la documentazione e degli atti (Deliberazioni, Determinazioni, Bandi di Gara, Bandi di Concorso, Regolamenti, ...) destinati alla pubblicazione all'interno dell'Albo Pretorio sul sito Web aziendale ai fini della loro massima diffusione.

Responsabili

I Responsabili del trattamento dei dati personali vengono designati con atto formale dal Titolare. Sono individuati fra i dipendenti a cui è stato conferito un incarico di:

Responsabilità di una unità organizzativa complessa (UOC)
Alta professionalità (AP) o unità operativa semplice (UOS) per strutture in Staff alla Direzione Generale

Sono inoltre individuati il Direttore Amministrativo ed il Direttore Sanitario quali responsabili dei trattamenti effettuati dalle proprie segreterie.

Il Responsabile del trattamento dei dati deve attenersi alle istruzioni, impartite dal Titolare nell'atto di nomina, nel presente regolamento od attraverso qualsiasi atto formale a valenza aziendale predisposto in campo privacy.

Il Responsabile collabora con il RAP:

Fornendo ogni informazione richiesta dalla stesso
comunicando tempestivamente ogni notizia rilevante ai fini della tutela della riservatezza
Comunicando tempestivamente l'inizio di ogni nuovo trattamento dei dati nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di responsabilità

Il Responsabile ha l'obbligo di nominare formalmente come incaricati le persone fisiche dipendenti o prestatori di lavoro e/o servizio a vario titolo dell'Azienda, che, nell'ambito dei trattamenti aziendali di propria diretta competenza, effettuano operazioni di trattamento di dati personali.

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al proprio settore di competenza.

La funzione di Responsabile del trattamento dei dati è attribuita personalmente e non è suscettibile di delega.

Incaricati

Il Responsabile del trattamento nomina quali incaricati le persone fisiche che nell'ambito dei trattamenti di loro diretta competenza effettuano materialmente operazioni di trattamento di dati personali.

Tale nomina costituisce presupposto di liceità per il trattamento dei dati personali e/o sensibili in ambito aziendale da parte di dette persone fisiche, siano esse dipendenti o prestatori di lavoro e/o servizio a vario titolo.

L'atto di nomina dell'incaricato contiene:

l'ambito dei trattamenti consentiti
eventuali ulteriori istruzioni a cui gli incaricati devono attenersi scrupolosamente nel trattare i dati personali – a complemento di quanto già stabilito all'interno di questo regolamento e di qualsiasi altro documento privacy aziendale
la prescrizione che gli incaricati abbiano accesso esclusivamente ai dati la cui conoscenza sia strettamente necessaria per l'espletamento dell'attività cui sono preposti

L'atto di nomina degli incaricati deve essere predisposto in forma scritta e contenere in allegato il Regolamento Aziendale Privacy vigente quale primo momento di informazione/formazione dell'incaricato.

Il Responsabile notifica l'atto di nomina al singolo incaricato e, per conoscenza, al RAP al quale comunica altresì le eventuali modifiche successivamente intervenute alla nomina degli incaricati.

Qualora il Responsabile debba designare più incaricati contemporaneamente si procede ad una sola designazione contenente più nominativi.

L'Azienda attua iniziative di formazione - misure minime - degli incaricati per consentire loro di acquisire conoscenze sulle modalità e sulla prassi operativa da tenersi per un corretto trattamento dei dati personali.

Responsabili Esterni

In tutti i contratti o convenzioni, con cui l'Azienda affida a terzi (Enti, organismi, associazioni di volontariato, persone fisiche, strutture private accreditate, società di persone o di capitali, studi legali, etc.) attività che comportano il trattamento di dati personali, deve essere inserita la clausola di garanzia con la quale il soggetto esterno si assume i seguenti obblighi:

Trattare i dati personali per le sole finalità necessarie all'espletamento delle attività ed ai conseguenti trattamenti oggetto dell'incarico ricevuto

Soddisfare gli obblighi previsti nel Codice Privacy

Rispettare i contenuti del Regolamento Privacy Aziendale e le eventuali specifiche prescrizioni previste per l'espletamento delle attività/servizi contrattualizzati

Informare sulle misure di sicurezza adottate (oltre che sulle eventuali successive modifiche) consentendone il monitoraggio da parte della Azienda Sanitaria

Informare immediatamente l'Azienda Sanitaria in presenza di situazioni anomale o di emergenze

Il Titolare od il Responsabile in possesso di delega, nomina, con atto formale - ai sensi dell'art. 29 del D.Lgs. 196/03 -, il soggetto terzo quale Responsabile Esterno dei trattamenti dei dati personali effettuati in forza del rapporto contrattuale o convenzionale e ne invia copia al RAP.

Il Responsabile Esterno deve individuare per iscritto le persone incaricate al trattamento e fornire loro le istruzioni relative alle operazioni da compiere. Deve inoltre vigilare sulla corretta osservanza delle istruzioni impartite provvedendo ad assicurare agli incaricati una adeguata formazione privacy.

Incaricati Esterni

Chiunque tratti dati in nome o per conto del Titolare deve essere nominato Incaricato: qualsiasi soggetto che a qualsiasi titolo sia autorizzato dalla struttura del Titolare a raccogliere, elaborare, utilizzare o consultare dati personali, risponde al profilo in questione sia che l'attività sia svolta dietro pagamento o a titolo puramente gratuito.

Per quanto sopra indicato il ruolo di Incaricato può essere assegnato anche ad un soggetto totalmente esterno (es.: stagista, componente di una associazione benefica).

L'individuazione dell'Incaricato Esterno segue le stesse modalità ed è sottoposta agli stessi vincoli previsti per la figura di incaricato.

Responsabile Esterno o Incaricato Esterno - Valutazione

In alcuni casi può sorgere il dubbio in merito all'eventualità di nominare il soggetto esterno come Incaricato o come Responsabile, in particolar modo, avendo riguardo alla quantità, al tipo e alla delicatezza, o meno, dei dati trasferiti o resi accessibili alla persona fisica esterna.

Ci si deve orientare verso la nomina a Responsabile (esterno) del trattamento quando la mole o la criticità di dati esternalizzati, nonché il tipo di attività da svolgere, sono tali da indurre a ritenere necessaria una maggiore responsabilizzazione del soggetto esterno, anche in ragione del maggiore tasso di autonomia operativa che può essergli concessa per via della sua particolare specializzazione (rispetto a quella concessa all'Incaricato, mero esecutore di compiti).

La nomina a Responsabile "esterno" necessita di un rapporto di collaborazione o di outsourcing caratterizzato da una certa continuità.

Il rapporto una tantum - in questo caso anche a prescindere dal "peso" del trattamento affidato - deve essere gestito tramite una nomina ad Incaricato ricorrendo all'apposizione di un termine specifico che comporti l'automatica decadenza dall'Incarico a prestazione ultimata.

Amministratori di Sistema

Gli Amministratori di Sistema sono le figure professionali:

- ❑ Che provvedono alla conduzione (gestione e manutenzione) di un sistema di elaborazione o delle sue componenti
- ❑ Gli amministratori di basi di dati
- ❑ Gli amministratori di reti e di apparati di sicurezza
- ❑ Gli amministratori di sistemi software complessi
- ❑ Coloro che si occupano della custodia delle credenziali e della gestione dei sistemi di autenticazione e di autorizzazione

Nell'espletamento delle loro attività tutte le figure sopra indicate sono "responsabili" di specifiche fasi lavorative ad elevata criticità - rispetto alla protezione dei dati personali - quali il salvataggio dei dati (backup/recovery), l'organizzazione e la manutenzione dei flussi di dati e di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware.

Queste mansioni comportano, in molti casi, l'accesso - con capacità estesa di potenziale intervento - ad informazioni "rilevanti", caratteristiche tali da dover sottoporre l'attività dell'amministratore di sistema a particolari vincoli normativi e regolamentari che, nel loro complesso, ne evidenziano la particolare capacità di azione e la conseguente natura fiduciaria delle relative mansioni.

Per tali motivazioni l'attribuzione delle funzioni di amministratore di sistema deve avvenire nel rispetto di una:

Valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato

Elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato

Indicazione degli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite (informazione da mantenersi in un documento interno aggiornato e disponibile in caso di accertamenti anche da parte del Garante). Tale prescrizione rimane valida anche nel caso di servizi di amministrazione di sistema affidati in outsourcing.

Costante e continuativa attività di verifica - da parte del Titolare o del RAP – destinata ad accertare la rispondenza delle misure organizzative, tecniche e di sicurezza alle norme ed ai regolamenti vigenti

Registrazione degli Accessi - Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono

avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo non inferiore a sei mesi.

Trattamenti

Oggetto del trattamento devono essere i soli dati essenziali per lo svolgimento delle attività istituzionali.

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato.

Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali lo stesso è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

E' compito dei Responsabili del trattamento verificare periodicamente la liceità e la correttezza dei trattamenti, 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 fornisca di propria iniziativa.

In ogni caso devono essere adottate misure organizzative, logistiche e tecniche tali da garantire che i dati personali o sensibili siano accessibili ai soli incaricati di trattamento e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

Il trattamento dei dati personali è ammesso solo da parte del Titolare del trattamento, dei Responsabili e degli incaricati. Non è consentito il trattamento di dati personali da parte di persone non autorizzate.

Il trattamento dei dati personali raccolti direttamente dalla ASL o ad essa comunicati da altri soggetti è effettuato nel rispetto del principi previsti dagli articoli 18, 19, 20 e 21 del Codice.

Il trattamento comprende, in particolare le seguenti operazioni sui dati: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, cancellazione, distruzione, comunicazione, diffusione.

I trattamenti effettuati dalla ASL sono finalizzati all'erogazione delle prestazioni sanitarie nonché agli adempimenti amministrativi e contabili, di organizzazione e di controllo preordinati alla predetta erogazione, con particolare riguardo alle attività di:

Prevenzione collettiva e di sanità
Diagnostica strumentale e di laboratorio
Prevenzione delle malattie, cura e riabilitazione in regime ambulatoriale territoriale sia in sede ospedaliera
Ricovero ordinario e di day hospital
Prestazioni sanitarie a rilevanza sociale
Controllo della salute dei lavoratori che operano all'interno dell'Ente

Sono inoltre effettuati i trattamenti di dati personali derivanti da norme legislative e regolamentari concernenti:

La gestione del personale dipendente, ivi comprese le procedure di assunzione
La gestione dei soggetti, che intrattengono rapporti giuridici con l'Ente diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Ente stesso, ivi compresi gli specializzandi, i docenti di corsi, i tirocinanti, i volontari

La gestione dei rapporti con i consulenti, i fornitori per l'approvvigionamento di beni e servizi nonché le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione
La gestione dei rapporti con i soggetti accreditati o convenzionati
La gestione dei rapporti con altri soggetti pubblici competenti per le attività ispettive di vigilanza, di controllo e di accertamento delle Infrazioni alle leggi ed ai regolamenti.

Trattamenti - Registro

Di seguito è riportato una elencazione – puramente esemplificativa ed assolutamente non esaustiva – dei trattamenti di dati personali effettuati all'interno della ASL di Lecce. Tale elenco costituisce il primo livello di implementazione della base dati (registro) che - a cura del RAP coadiuvato dall'Ufficio Privacy - dovrà essere costantemente aggiornata attraverso le segnalazioni, inviate allo stesso, dai Responsabili individuati riguardanti trattamenti non presenti in elenco e/o modifiche di trattamenti già censiti e/o cancellazione di trattamenti non più effettuati.

L'aggiornamento costante dell'elenco dei trattamenti è fondamentale per consentire l'individuazione formale degli incaricati attraverso l'associazione "responsabili - trattamenti - incaricati individuati" effettuata utilizzando la modulistica proposta in allegato da utilizzarsi per detta formalizzazione.

Elenco trattamenti:

- Assistenza sanitaria di base: riconoscimento del diritto all'esenzione per patologia/invalidità/reddito/malattie rare/grandi invalidi e gestione archivio esenti
- Assistenza ai nefropatici cronici in trattamento dialitico
- Assistenza domiciliare programmata e integrata
- Assistenza integrativa fornitura di prodotti dietetici a categorie particolari
- Assistenza integrativa fornitura di presidi sanitari a soggetti affetti da diabete mellito
- Assistenza protesica
- Assistenza sanitaria di base: assistenza agli stranieri in Italia (particolari categorie)
- Assistenza sanitaria di base: assistenza sanitaria in forma indiretta
- Assistenza sanitaria di base: cure all'estero
- Assistenza specialistica ambulatoriale e riabilitazione
- Assistenza termale
- Attività medico - legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale
- Attività medico - legale inerente l'istruttoria delle richieste di indennizzo per danni da vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati
- Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
- Attività medico - legale inerente l'accertamento dell'idoneità al porto d'armi, ai fini della sicurezza sociale

- Attività medico - legale inerente l'accertamento dell'idoneità in ambito di diritto al lavoro (assunzione nel pubblico impiego; idoneità allo svolgimento di mansioni lavorative; controllo dello stato di malattia di dipendenti pubblici e privati)
- Attività amministrativa, programmatoria, gestionale e di valutazione relativa alla assistenza in regime di ricovero ospedaliero e domiciliare
- Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'attività immuno-trasfusionale
- Attività amministrativa, programmatoria, gestionale e di valutazione concernente il trapianto d'organi
- Attività di assistenza riabilitativa residenziale e semiresidenziale ad anziani non autosufficienti, disabili psichici e sensoriali e malati terminali
- Attività fisica e sportiva
- Attività medico - legale in ambito necroscopico
- Attività medico - legale inerente gli accertamenti finalizzati al sostegno delle fasce deboli (riconoscimento dello stato di invalidità civile, cecità civile, sordomutismo, della condizione di handicap, accertamenti per il collocamento mirato al lavoro delle persone disabili)
- Attività sanzionatoria e di tutela amministrativa e giudiziaria
- Consulenze e pareri medico-legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari
- Consulenze e pareri medico-legali in tema di riconoscimento della dipendenza da causa di servizio
- Dipendenze (tossicodipendenze e alcool dipendenze)
- Gestione attività sociosanitaria a favore di fasce deboli di popolazione
- Gestione dei rapporti di lavori del personale inserito a titolo differente nella ASL, collocamento obbligatorio, assicurazioni integrative
- Gestione e verifica dell'attività specialistica e di ricovero per le strutture accreditate
- Medicina di base - pediatria di libera scelta - continuità assistenziale (guardia medica notturna e festiva, guardia turistica)
- Nomine e designazioni
- Programmi di diagnosi precoce
- Promozione e tutela della salute mentale
- Soccorso sanitario di emergenza/urgenza "118" ed assistenza sanitaria di emergenza
- Sorveglianza epidemiologica delle malattie infettive e diffusive e delle tossinfezioni alimentari
- Tutela dai rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro
- Vaccinazioni e verifica assolvimento obbligo vaccinale
- Videosorveglianza con finalità di sicurezza e protezione di beni e persone

Informativa

L'informativa è l'elemento propedeutico al trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere.

L'informativa è sempre dovuta a prescindere dall'obbligo di acquisizione del consenso. Essa deve contenere gli elementi tassativamente indicati dall'art. 13 del D.Lgs. 196/03 e più specificatamente:

Le finalità e le modalità con le quali vengono 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 o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi
I diritti di cui al paragrafo
Gli estremi identificativi del Titolare e del RAP
Indicazione della specifica sezione del portale web aziendale in cui sono elencati i Responsabili Aziendali del trattamento

L'informativa può essere resa anche tramite affissione di appositi manifesti nei locali di accesso all'utenza, secondo procedure (es: avvertenze inserite nei documenti di affidamento di incarico e/o servizio) e attraverso modelli da rendere disponibili all'utenza validati dal RAP.

Al personale dipendente, al personale medico convenzionato, ai soggetti con i quali vengono instaurati rapporti di collaborazione libero-professionali, agli specializzandi, ai tirocinanti, ai docenti di corsi, ai volontari, agli operatori del servizio civile ecc., l'informativa viene fornita per iscritto in sede di instaurazione dei relativi rapporti (Area Personale – Ufficio Formazione) in uno con l'ultima versione disponibile del presente Regolamento.

Ai soggetti che hanno già instaurato rapporti con l'Ente, l'informativa è fornita nei tempi e con modalità che saranno concordate tra il RAP ed i Responsabili del trattamento.

Alle ditte partecipanti a gare di forniture di beni o servizi o di affidamento di lavori, ai candidati di concorsi o di avvisi pubblici l'informativa viene resa in sede di pubblicazione dei relativi bandi.

Diritti dell'Interessato

Secondo quanto disposto dall'art. 7 del D.Lgs. 196/03, l'interessato ha diritto di ottenere a cura del Titolare o del Responsabile:

- La conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile
- L'indicazione:
- dell'origine dei dati personali trattati
- delle finalità e delle modalità del trattamento
- della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici
- degli estremi identificativi del Titolare
- dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati

Ha inoltre diritto a che Il Titolare od il Responsabile garantiscano:

a) L'aggiornamento, la modifica ovvero, qualora vi abbia interesse, l'integrazione dei dati
b) La cancellazione, trasformazione in forma anonima, 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 ai precedenti punti a) ed 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 riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato

L'interessato ha inoltre il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

L'interessato, nell'esercizio dei diritti sopra riportati, può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni

Diritto di Accesso

Con Deliberazioni del Direttore Generale n. 790 del 05/03/2009 e 2564 del 31/07/2009, è stato approvato il regolamento di accesso agli atti che disciplina le modalità ed i casi di esclusione dell'accesso ai documenti amministrativi ed alle cartelle cliniche in conformità all'art. 24 della Legge 7 agosto 1990 n. 241.

Tale regolamentazione deve trovare applicazione nel rispetto delle prescrizioni imposte in tal senso dal Codice Privacy.

In particolare, per quanto attiene la documentazione sanitaria, ai sensi dell'art. 92 del Codice Privacy, eventuali richieste di presa visione o di rilascio di copia della cartella clinica ed, eventualmente, della scheda di dimissione ospedaliera, da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile

Le richieste di accesso di un terzo diverso dal soggetto interessato alle cartelle cliniche sono valutate dal Direttore Medico del Presidio Ospedaliero che ne ha la responsabilità applicando i criteri enunciati nel capoverso che precede. Ai fini del bilanciamento degli interessi potrà essere chiesto parere al RAP.

Tutta la documentazione sanitaria (non solo la cartella clinica) può essere ritirata anche da persona diversa dal diretto interessato solo in presenza di una delega scritta e mediante consegna dei documenti in busta chiusa.

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo attraverso le forme previste dall'art. 84 del Codice Privacy (medico designato dall'interessato o dal titolare ovvero esercente la professione sanitaria specificamente incaricato dal Titolare).

Misure di Sicurezza

Per misure di sicurezza devono intendersi l'insieme delle prescrizioni di carattere tecnico, tecnologico, procedurale logistico ed organizzativo finalizzate all'implementazione del livello minimo di sicurezza per il trattamento dei dati personali.

Accesso alle Aree ed ai Locali

I Responsabili del trattamento vigilano affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati e/o vengono trattati dati personali.

L'installazione di apparecchiature di video-sorveglianza è autorizzata dal Titolare del trattamento dei dati - sentito il RAP - previo accordo con le organizzazioni sindacali, solo quando ciò sia strettamente indispensabile per l'esercizio delle attività assistenziali, ovvero per la sicurezza delle persone e delle attrezzature e non siano attuabili o sufficienti altre misure di sorveglianza come meglio indicato nel paragrafo .

I Responsabile hanno inoltre il compito di:

- ❑ Predisporre appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere
- ❑ Predisporre soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rilevare lo stato di salute

Il trattamento di dati sensibili e/o giudiziari contenuti in documenti cartacei avviene per il tempo strettamente necessario al trattamento, con successiva immediata archiviazione dei dati. L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari avviene in locali ad accesso controllato, utilizzando armadi, cassetti e porte chiusi a chiave.

Trattamenti effettuati senza l'ausilio di strumenti elettronici

Il trattamento dei dati senza strumenti elettronici è effettuato utilizzando i dati contenuti in tutti i supporti cartacei o simili che, in ogni caso, non richiedano e/o non facciano uso, di elaboratori elettronici.

La gestione degli archivi cartacei ricade nella competenza del Responsabile del trattamento che discrimina - tra i documenti da archiviarsi - le tipologie contenenti dati sensibili e/o giudiziari.

Il Responsabile assicura che la documentazione venga custodita in armadi o in locali dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato ed individua tra i dipendenti gli incaricati di tale attività.

Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.

In particolare, per i trattamenti che prevedono l'uso di dati contenuti nelle cartelle cliniche, per le stesse deve essere attuato una tecnica di anonimizzazione riportando sul frontespizio il solo numero nosologico, trasferendo, di conseguenza i dati anagrafici e clinici all'interno.

Custodia

I documenti contenenti dati personali sono custoditi in modo da non essere accessibili alle persone non incaricate dello specifico trattamento attraverso il deposito degli stessi in locali e spazi che prevedono un accesso riservato (es. locali e stanze, armadi e cassetti chiusi a chiave).

I documenti sono prelevati dal personale incaricato dagli archivi per l'attività quotidiana e quivi ricollocati al termine della giornata.

Nell'espletamento dell'attività legata all'incarico i documenti contenenti dati personali non devono rimanere Incustoditi su scrivanie o tavoli da lavoro

Laddove l'espletamento dell'incarico preveda rapporti con l'utenza si deve avere cura di tenere in vista solo la documentazione che attiene al solo interessato con il quale si sta interagendo.

Selezione, scarto e distruzione

La selezione e lo scarto della documentazione avvengono nel rispetto delle prescrizioni normative vigenti e della regolamentazione aziendale sul massimario di scarto – D.D.G. 3651 del 07.12.2010 e D.D.G. 348 del 11.02.2011.

La distruzione di grandi quantità di documentazione contenenti - anche - dati personali è effettuata nel rispetto di quanto previsto dalla specifica regolamentazione interna e/o dalle procedure implementate da aziende esterne a cui è stato affidato lo specifico servizio. In ogni caso le modalità utilizzate devono essere tali che venga impedita qualsiasi ricomposizione del singolo documento.

Tali prassi operative devono essere mantenute da parte di ogni singolo incaricato anche per la distruzione di tutta la documentazione prodotta in copia e/o come parziale riproduzione dell'originale ai fini dell'espletamento dell'attività oggetto dell'incarico (appunti, fotocopie di lavoro, ...).

Comunicazione

Vige il vincolo per il quale i dati personali non devono essere condivisi, comunicati o inviati a personale, soggetti terzi e istituzioni che non condividono lo specifico trattamento e/o ne abbiano bisogno per lo svolgimento delle funzioni lavorative.

I dati non devono essere comunicati all'esterno della struttura e comunque a terzi se non previa autorizzazione.

In particolare la comunicazione di dati personali ad altri soggetti pubblici è ammessa solo quando sia prevista da una norma di legge o di regolamento (art. 19, comma 2, D.Lgs. 196/03). In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali.

La comunicazione di dati personali a privati e la diffusione sono ammesse unicamente quando siano previste da una norma di legge o di regolamento (art. 19, comma 3 D.Lgs. 196/03).

I dati idonei a rivelare lo stato di salute non possono essere diffusi (art. 22, comma 8 D.Lgs. 196/03).

Trattamenti effettuati con l'ausilio di strumenti elettronici

Sicurezza Informatica

La sicurezza informatica per i trattamenti effettuati con l'ausilio di strumenti elettronici deve essere perseguita attraverso l'applicazione di *policy di sicurezza* stabilite aziendalmente ed applicate a livello *centrale* e *periferico*.

L'implementazione delle *policy di sicurezza* a livello *centrale* è di competenza dell'organizzazione - interna od in outsourcing - che si occupa della gestione dei sistemi informativi: la definizione delle politiche di sicurezza spetta all'Unità Organizzativa "Amministrazione Digitale Sicurezza e Privacy" che procede in tal senso in collaborazione con l'Unità Organizzativa "Sistemi Informativi Aziendali".

Tutta la documentazione elaborata - oltre ad interpretarsi in combinato disposto con il documento di che trattasi - deve garantire la *conformità privacy* sia rispetto alla normativa nazionale sia rispetto alla regolamentazione aziendale anche ed in particolare riguardo l'organizzazione e le prassi operative per:

Le modalità per il ripristino della disponibilità dei dati
La custodia e l'uso dei supporti rimovibili/distruzione supporti rimovibili
La prevenzione dei virus informatici
La politica di aggiornamento software

Gli esiti dell'applicazione delle policy di sicurezza centrali - in buona parte trasparenti alla utenza aziendale - hanno ricadute a livello *periferico* rispetto all'attività del singolo incaricato e possono essere riassunte - conformità privacy - negli elementi di seguito proposti.

Custodia delle stazioni di lavoro

La stazione di lavoro non deve essere lasciata incustodita ed accessibile a terzi durante una sessione di trattamento.

Sulla stazione di lavoro devono essere attivati key locks o screensaver - protetti con password di ripristino - che si devono attivare su richiesta o entro un tempo massimo di inattività pari a tre minuti - laddove esista la necessità di allontanarsi temporaneamente dalla stessa.

Al termine delle sessioni di lavoro su applicati centralizzati o comunque remoti, effettuare la procedura di disconnessione (log off/ log out).

Al termine della quotidiana attività effettuare la procedura di arresto della stazione di lavoro prima di allontanarsi dall'ufficio.

Credenziali delle stazioni di lavoro e degli applicativi

Le credenziali di autenticazione sono univoche ed associate al singolo utente e non possono essere nuovamente assegnate ad un altro soggetto.

Gli incaricati del trattamento ricevono istruzioni sulle modalità di utilizzo delle credenziali di autenticazione o nel momento dell'assegnazione (attivazione) o, in termini generali, all'interno della documentazione aziendale sulle policy di sicurezza.

L'incaricato è tenuto a modificare la propria password dopo un periodo non superiore ai 60 giorni.

La nuova password dovrà essere composta da almeno dieci caratteri alfanumerici, con la presenza di almeno due numeri ed eventualmente con una successione di lettere minuscole e maiuscole.

I contenuti informativi della nuova password non devono essere direttamente associabili all'incaricato (sottoinsieme del codice fiscale, nome e data di nascita, nome del figlio e della figlia, ...).

La password dovrà essere custodita accuratamente ed ovviamente non dovrà essere né comunicata né divulgata neanche per consentire l'espletamento delle attività istituzionali in periodi di assenza dell'incaricato per malattia, ferie, ...

Il Responsabile del trattamento è tenuto ad informare il responsabile dell'Unità Organizzativa "Amministrazione Digitale Sicurezza e Privacy" e/o il responsabile dell'Unità Organizzativa "Sistemi Informativi Aziendali" laddove l'incaricato abbia cessato per qualsiasi motivazione (pensionamento, cambio di unità operativa, malattia, ...) l'attività al fine di revocare le specifiche credenziali per l'accesso.

Le credenziali di accesso non utilizzate per un periodo superiore ai sei mesi saranno revocate d'ufficio.

Misure Minime

Le misure di sicurezza sono costituite dal complesso delle misure organizzative, tecniche, informatiche, logistiche e procedurali volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta, modifica dei dati in conseguenza di interventi non autorizzati o non conformi alla regole.

L'obbligo di adozione annuale del documento programmatico sulla sicurezza è stato revocato: al suo posto verrà redatto - a cura del RAP e dell'Ufficio Privacy - un documento programmatico sulla sicurezza semplificato - DPSS - costantemente aggiornato, avente il compito di garantire a livello aziendale il massimo livello di conoscenza e trasparenza in merito alle misure privacy vigenti.

Tutti i titolari di trattamento sono tenuti ad adottare misure minime individuate dal Codice e secondo le modalità previste nel Disciplinare tecnico allegato al Codice.

E' fondamentale sottolineare che non viene fatta differenza tra violazione della riservatezza dei dati personali - accesso a dati sensibili da parte di terzi non autorizzati - e distruzione o perdita accidentale di dati già legittimamente raccolti e trattati: il responsabile di questo danno è sanzionato.

Per questi motivi il soggetto che non adotta misure di sicurezza può essere sanzionato penalmente (nel caso in cui non siano state rispettate le misure minime) e può essere chiamato a rispondere civilmente per il risarcimento del danno (nel caso in cui non si siano implementate misure idonee).

Le misure di sicurezza adottate per il trattamento dei dati personali devono essere:

- ❑ adeguate in relazione alle conoscenze acquisite in base al progresso tecnico e tali da ridurre al minimo i rischi di distruzione dei dati o accesso non autorizzato
- ❑ adottate in via preventiva e differenziate in base alla natura dei dati e alle specifiche caratteristiche del trattamento.

Differenza tra misure minime e misure idonee

Il titolare deve individuare preventivamente misure di sicurezza che devono almeno rispettare i parametri di sicurezza minimi individuati nel Codice (articoli 33, 34, 35 e 36) e nel Disciplinare Tecnico (Allegato B del Codice Privacy).

Se le misure di sicurezza adottate non rispettano i parametri minimi contenuti nel regolamento, si concretizza la fattispecie penale di omissione delle misure minime e la conseguente responsabilità.

L'individuazione di misure che rispettano i parametri previsti come minimi non è sufficiente a liberare da ogni responsabilità il soggetto che effettua il trattamento: se le misure adottate non sono idonee ad evitare il danno, il Titolare può essere coinvolto comunque sotto un profilo di responsabilità civile, anche se non ci sono gli estremi per la responsabilità penale prevista dalla legge.

Nel caso le misure adottate non siano idonee ad evitare il danno l'articolo 15 del Codice Privacy rimanda all'articolo 2050 del Codice Civile (relativo allo svolgimento di attività pericolose con onere dell'inversione della prova).

Le conseguenze della mancata adozione di misure di sicurezza porta ad una sanzione penale per omessa adozione con arresto sino a due anni ovvero ad un risarcimento del danno.

Formazione Privacy

La formazione in campo privacy è una delle iniziative da intraprendersi per il soddisfacimento delle misure minime di sicurezza. La norma prescrive che il dipendente neo assunto sia sottoposto a formazione ancora prima di cominciare ad espletare i suoi compiti istituzionali.

In assenza di tale – reale – opportunità il processo di formazione per il personale dipendente deve essere costante e continuativo.

Oltre alle iniziative classiche di formazione in aula – che in presenza di vincoli dimensionali quali quelli aziendali – sono intrinsecamente limitatamente efficaci, è possibile prevedere iniziative di formazione in FAD – Formazione a Distanza – da erogarsi presso le postazioni PC dei dipendenti e la fruizione di documentazione specifica quali regolamentazione, FAQ, casi di studio, modelli, ..., sia in forma cartacea sia elettronica.

E' opportuno prevedere l'erogazione di specifica e approfondita formazione ai Responsabili individuati – chiamati, oltre che ad interagire con il RAP anche a rendere possibile il processo di diffusione informativa nei confronti degli incaricati della struttura organizzativa.

Documento Programmatico sulla Sicurezza Semplificato – DPSS

Pur essendo decaduto l'obbligo della redazione annuale del Documento Programmatico sulla Sicurezza - DPS, la tenuta di un Documento Programmatico sulla Sicurezza Semplificato – DPSS costantemente riveduto ed aggiornato, è da intendersi come adozione di una misura di sicurezza opportuna e strategica.

Il DPSS è, di fatto, il contenitore informativo privacy aziendale dovendo confluire nello stesso - al minimo – i dati relativi a:

- ❑ Titolare - Dati Identificativi
- ❑ RAP e Ufficio Privacy - Dati Identificativi - Costituzione - Compiti
- ❑ Responsabili - Dati Identificati ed elenco dei trattamenti associati
- ❑ Elenco dei Trattamenti - Finalità - Interessati - Modalità - Misure di Sicurezza
- ❑ Incaricati - Trattamenti Associati – Responsabilità
- ❑ Misure di Sicurezza Generali

Nel DPSS confluiscono le informazioni del Registro dei Trattamenti implementato con l'aiuto dei Responsabili insieme alle ulteriori notizie in merito ai trattamenti che gli stessi forniscono (incaricati-modalità - ..).

Nello specifico il raccordo funzionale con i Responsabili individuati, con "Sistemi Informativi" e con "Amministrazione Digitale" sono propedeutici ad una efficace predisposizione del documento, in particolare, rispetto al suo costante aggiornamento.

Videosorveglianza

Principi Generali

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (art. 4, comma 1, lett. b), del Codice). È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati.

L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in particolare in materia di interferenze illecite nella vita privata e sul controllo a distanza dei lavoratori.

In tale quadro, pertanto, è necessario che:

- ❑ Il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente (svolgimento di funzioni istituzionali: artt. 18-22)
- ❑ Il sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone)
- ❑ L'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom - trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite - (art. 11, comma 1, lett. d) del Codice)

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata. A tal fine, il Garante ritiene che si possa utilizzare lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita:

In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.

Figura 1

Figura 2

Il supporto con l'informativa (figura 1):

- ❑ Deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti
- ❑ Deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno
- ❑ Può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione (figura 2), eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Misure di Sicurezza

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche

accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

In relazione alle finalità perseguite ed alla possibile varietà dei sistemi tecnologici utilizzati, le misure minime di sicurezza possano variare anche significativamente ma devono comunque essere quanto meno rispettose dei principi che seguono:

- In presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza
- Laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione
- Per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto
- Nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele (accesso alle immagini solo se strettamente indispensabile)
- Qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale
- La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza

Responsabili ed Incaricati

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (art. 30 del Codice). Deve trattarsi di un numero circoscritto di soggetti, specie quando il titolare si avvale di collaboratori esterni.

Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento (art. 29 del Codice).

Durata della Conservazione

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (v. art. 11, comma 1, lett. e) del Codice), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita.

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici

o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di scadenza dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

Rapporti di Lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (telecamera sul badge).

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della Legge n. 300/1970, gli impianti e le apparecchiature, "dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori", possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali.

Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro.

Ospedali e Luoghi di Cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione, reparti di isolamento), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.

Devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione di quanto prescritto dal provvedimento generale del 9 novembre 2005 adottato in attuazione dell'art. 83 del Codice13.

Il titolare deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico).

Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.

Va assolutamente evitato il rischio di diffusione delle immagini di persone malate su monitor collocati in locali liberamente accessibili al pubblico.

Sistemi Integrati di Videosorveglianza

Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

- ❑ Gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime *infrastrutture tecnologiche → trattamento delle immagini solo nei termini strettamente funzionali* al perseguimento dei compiti istituzionali
- ❑ Collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo (service) → il soggetto terzo è designato responsabile del trattamento ed assume un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire forme di correlazione delle immagini raccolte per conto di ciascun titolare

Sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati.

Portale Web Aziendale

Uno degli ambiti maggiormente interessati dalle potenziali ricadute della mancata osservanza delle prescrizioni privacy è - evidentemente - Internet in tutte le sue declinazioni informative.

La normativa nazionale (Trasparenza Amministrativa – Codice dell'Amministrazione Digitale – Semplificazione Amministrativa - ...) pone sempre più enfasi sugli aspetti legati alla conoscibilità dell'attività della Pubblica Amministrazione da parte del cittadino utente.

Uno degli strumenti più potenti – in tal senso – è l'Albo Pretorio On-Line, ovvero della possibilità di rendere disponibile quanto in precedenza pubblicato in forma cartacea alla bacheca aziendale, al mondo intero in formato elettronico.

Il Garante Privacy – consapevole sia dei rischi derivanti da un così potenzialmente vasto ambito di diffusione informativa sia della conseguente necessità di innalzare il livello di attenzione delle PA rispetto la corretta applicazione delle prescrizioni privacy – si è più volte espresso in tal senso sia con Pareri che con Provvedimenti. Ha inoltre pubblicato le "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute" ed ha avallato il documento redatto dal Ministero delle Pubblica Amministrazione e l'Innovazione "Linee Guida per i Siti delle PA".

Il processo di pubblicazione - potenzialmente di qualsiasi informazione e documentazione prodotta aziendalmente – deve naturalmente tenere conto di tali elementi e prescrizioni.

La "revisione finale privacy" deve essere effettuata a valle dell'intero processo di produzione del documento in un momento immediatamente antecedente a quello della "pubblicazione web" quando lo stesso ha già

sostenuto la verifica di conformità amministrativa e di contenuto (come meglio esplicitato nel paragrafo "Processo di Pubblicazione").

Non potendosi prevedere l'analisi di tutta la documentazione e degli atti prodotti aziendalmente l'Ufficio Privacy – oltre a fornire consulenza e formazione – avrà il compito di alimentare la base dati relativa ai "casi di studio" ed alle "domande più frequenti - FAQ" per macro tipologia di situazione e di documentazione.

Tale base di dati – assieme a quella relativa alla modulistica – sarà costantemente alimentata e messa a disposizione aziendalmente con tutti i possibili mezzi diffusione interna.

Modulistica

La redazione e standardizzazione della modulistica (informative, consenso al trattamento, cartelloni informativi, ...) è una ulteriore attività privacy per la tenuta delle misure minime di sicurezza. Il disallineamento della documentazione in utilizzo presso strutture omologhe e/o la inadeguata predisposizione dei modelli in uso – in particolare note informative e moduli di consenso – pur se frutto di eredità amministrative ed organizzative - può determinare situazioni paradossali e contraddizioni in termini e fatti all'interno della stessa azienda.

Anche in questo caso il compito deve essere assolto dall'Ufficio Privacy che, oltre alla predisposizione della cartellonistica generale e della modulistica "base", contribuisce alla definizione della modulistica personalizzata – assieme ai responsabili - per le diverse tipologie di unità operativa e trattamento – così come intrinsecamente prevede la norma –.L'Ufficio Privacy deve ottemperare al compito ponendo quella particolare cura e professionalità atta ad evitare – oltre alle sanzioni del Garante – lesioni della sfera privata del cittadino e del personale aziendale.

Documentazione

Di seguito viene proposto l'elenco della documentazione aziendale che, – oltre che per la sua valenza amministrativa e strategica – in ottemperanza alla normativa vigente, deve essere pubblicata sul Portale Web Aziendale:

- ❑ Deliberazioni
- ❑ Determinazioni
- ❑ Documentazione relativa a Gare
- ❑ Documentazione relativa a Concorsi
- ❑ Dati informativi sull'organizzazione e i procedimenti
- ❑ Dati informativi relativi al personale
- ❑ Dati relativi a incarichi e consulenze
- ❑ Dati sulla gestione economico-finanziaria
- ❑ Dati relativi alle buone prassi
- ❑ Dati su sovvenzioni, contributi, crediti, sussidi e benefici di natura economica

Processo di Pubblicazione

Partendo dai presupposti che solo una parte residuale degli atti aziendali è totalmente endogeno, che quasi tutti gli atti contengono dati personali e/o sensibili e che l'attività di pubblicazione sul portale aziendale degli atti destinati alla diffusione è solo l'ultimo dei passaggi operativi necessari alla formazione compiuta della documentazione, la conformazione alle prescrizioni privacy della stessa deve essere vista come un processo che si innesca nel momento stesso in cui si forma l'atto.

E' quasi sempre necessario produrre due versioni dello stesso documento: la prima – destinata all'utilizzo interno – totalmente "in chiaro"; la seconda – destinata alla diffusione su web - adeguatamente privatizzata. Non possono essere definite modalità di intervento valide - a prescindere - per qualsiasi atto, ma la privatizzazione deve essere frutto dell'applicazione attenta – da parte del redattore adeguatamente formato – di regole generali.

Il percorso, stante la numerosità della documentazione prodotta, la diversità delle tipologia di atto, il diverso grado di conoscenza della normativa e conseguente conformazione alle prescrizioni dei redattori, la potenziale dirompenza degli esiti di una mancata adozione di misure minime di sicurezza (per lo specifico), l'intervento di "revisione finale privacy" da parte dell'Ufficio Privacy, costituisce elemento di garanzia per tutta la filiera di produzione dell'atto (redattore – istruttore – avallatore – sottoscrittore - autorizzatore) – responsabile a vario titolo e grado – della conformità dello stesso.

Casi di Studio – Domande più Frequenti - FAQ

Non potendosi prevedere l'analisi di tutta la documentazione e degli atti prodotti aziendalmente l'Ufficio Privacy – oltre a fornire consulenza e formazione – avrà il compito di alimentare la base dati relativa ai "casi di studio" ed alle "domande più frequenti - FAQ" per macro tipologia di situazione e di documentazione.

Tale base di dati – assieme a quella relativa alla modulistica – sarà costantemente alimentata e messa a disposizione aziendalmente con tutti i possibili mezzi diffusione interna.

Sistemi Informativi - Amministrazione Digitale

Fondamentale – rispetto all'ambito ed alle modalità di applicazione – è l'interazione del RAP con i responsabili delle strutture responsabili dei Sistemi Informativi e dell'applicazione dei contenuti del Codice dell'Amministrazione Digitale e delle norme che trattano della "Semplificazione Amministrativa" – Amministrazione Digitale e di ciò che riguarda la sicurezza logica del sistema informativo.

Per tutto ciò che riguarda i trattamenti effettuati con l'utilizzo di strumentazione elettronica qualsiasi iniziativa in ambito di privatizzazione deve essere – propedeuticamente - concordata ed eventualmente intrapresa con dette strutture in maniera da renderla trasparente ed efficace.

Diffusione Informativa ed Accesso

Il RAP concorda con i responsabili dei Sistemi Informativi e dell'applicazione dei contenuti del Codice dell'Amministrazione Digitale modalità organizzative e tecniche al fine di consentire le migliori condizioni di diffusione informativa ed accesso all'intero set di documentazione privacy predisposto aziendalmente.

In particolare la fruizione sarà garantita attraverso le funzionalità di gestione documentale e di contenuti alla specifica sezione informativa del Portale Intranet Aziendale all'indirizzo http::/intranet/.

IL DIRETTORE GENERALE

Vista la relazione istruttoria del dottore Cappelluti Tasti

Viste le sottoscrizioni poste in calce al presente provvedimento da parte del Responsabile dell'istruttoria

Acquisito il parere favorevole del Direttore Amministrativo e del Direttore Sanitario;

DELIBERA

- **Approvare** l'allegato "Regolamento per la Protezione dei Dati Personali - D.Lgs. 196/03 - Codice Privacy"
- **Individuare** il Responsabile Aziendale Privacy nella persona del dottor Antonio Cappelluti Tasti già dirigente responsabile dell'unità Amministrazione Digitale, Sicurezza e Privacy
- **Individuare** in qualità di Responsabili Privacy i titolari di incarico di unità organizzativa complessa (UOC), alta professionalità (AP) o unità operativa semplice (UOS) per strutture in staff alla Direzione Generale, nonché il Direttore Amministrativo ed il Direttore Sanitario limitatamente ai trattamenti effettuati dalle rispettive segreterie
- **Istituire** l'"Ufficio Privacy" assegnando allo stesso i compiti previsti nel Regolamento
- **Demandare** alla Direzione Amministrativa l'individuazione del personale - funzionalmente e gerarchicamente dipendente - necessario per l'espletamento dei compiti dell'Ufficio anche al fini di completare l'organico della struttura Amministrazione Digitale, Sicurezza e Privacy
- **Individuare** il Portale Intranet Aziendale quale strumento di elezione per la messa in disponibilità e diffusione delle iniziative e dei contenuti privacy all'interno della azienda
- **Attivare** il processo di rilevazione dei trattamenti effettuati e l'individuazione formale degli incaricati con la contestuale implementazione del registro elettronico da parte dell'Ufficio Privacy
- **Assoggettare** al processo di "revisione privacy" - in forma propedeutica alla pubblicazione - tutti gli atti e documenti aziendali destinati alla diffusione "erga omnes" - *sino al completamento del processo di in/formazione dei dirigenti per "Privacy" e "Trasparenza", alla diramazione di speciali atti di vincolo ed alla formalizzazione dello specifico Regolamento per l'individuazione dei compiti e per la delega di responsabilità nel processo di pubblicazione dei documenti aziendali* -
- **Attivare,** da parte dell'Ufficio Privacy, il processo di revisione ed uniformazione delle misure privacy sino ad ora intraprese con particolare riguardo a modulistica, gestione strumentazione elettronica, video sorveglianza
- **Trasmettere** il presente provvedimento a tutti i titolari di incarico di unità organizzativa complessa (UOC), alta professionalità (AP) o unità operativa semplice (UOS) per strutture in staff alla Direzione Generale
- **Pubblicare** il "Regolamento per la Protezione dei Dati Personali - D.Lgs. 196/03 - Codice Privacy" sul Portale Aziendale Internet nella sezione Regolamenti

Istruttori

Dottore Antonio Cappelluti Tasti .....

Il Direttore Amministrativo
Dott. Antonio Vigna .....

FIRMATO
Dott. Antonio VIGNA

Il Direttore Sanitario
Dott.Ottavio Narracci .....

FIRMATO
(Dott. Ottavio NARRACCI)

Il Direttore Generale
Dott. Valdo Mellone .....

FIRMATO
Dott. Valdo MELLONE

AZIENDA SANITARIA LOCALE
LECCE

n. _____ Reg. pubbl.

La presente Deliberazione è pubblicata per 15 giorni consecutivi all'Albo Pretorio aziendale nonché sul Sito Web Istituzionale , nella pagina relativa alla **Asl di Lecce** del Portale Regionale della Salute **www.sanita.puglia.it**

dal 12 LUG. 2013 al 26 LUG. 2013

Lecce, lì 12 LUG. 2013

Il Responsabile della Pubblicazione

FIRMATO
Dott.ssa Luigia Sonia Cioffi

La presente Deliberazione è trasmessa al Collegio Sindacale.