AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Studio Reginelli

Corso 196/03 per i Responsabili e gli Incaricati del Trattamento Dati

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Percorso Formativo per l'Incaricato del Trattamento Dati:

- Pre-requisiti:
  1. Conoscenza dei dati trattati
  2. Conoscenza degli strumenti utilizzati
  3. Conoscenza del proprio ruolo all'interno della struttura
- Obiettivi:
  1. Conoscenza elementare della normativa sul trattamento dati
  2. Sensibilizzazione alle problematiche di sicurezza dati
  3. Obblighi e sanzioni connessi al trattamento dati
  4. Motivazione alla partecipazione al "progetto privacy"

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Unità Didattica – 1 Quadro Normativo

1. Legge 23/12/93 n° 547 "Modifiche norme del codice penale in tema di criminalità informatica"
2. D.Lgs. 196/03 "Codice privacy"
3. Allegato B: "misure minime"
4. Reattività del sistema rispetto alle sollecitazioni esterne

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Unità Didattica – 2 La Sicurezza dei Dati

1. Risorse, minacce, rischi
2. Le contromisure
   - Misure di sicurezza fisica, elettronica, procedurale
   - Strumenti di protezione *hardware* e *software*
3. Il piano di *disaster recovery*
4. Raccomandazioni tecniche

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Progetto Privacy

A: Informative e consensi	B: Piano di sicurezza informatico	C: Formazione
Dipendenti Clienti Utenti Fornitori Altro	Rilevazione patrimonio informativo Classificazione dati, hardware e software *"Stato dell'arte"* Linee guida Formalizzazione dei ruoli Analisi dei rischi Misure minime Misure Idonee Notifica DPS	Titolare Responsabile Incaricato

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Legge 23/12/93 n° 547 "Modifiche norme del codice penale e del codice di procedura penale in tema di criminalità informatica"

- La Criminalità Informatica
- Risvolti Penali relativi al Trattamento dei Dati

AZIENDA OSPEDALIERA UNIVERSITARIA S.U.N.

LA CRIMINALITÀ INFORMATICA

L'introduzione di sanzioni penali conseguenti a:

- Accesso abusivo ad un sistema informatico o telematico
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

D.Lgs. 196/03 "Codice privacy"

- Principi fondamentali
- Figure coinvolte nel trattamento dei dati personali
- La raccolta ed i requisiti dei dati
- I diritti dell'interessato
- Il trattamento dati "particolari"
- Le sanzioni e i profili di responsabilità

Principi fondamentali

- Art. 1: "*Chiunque ha diritto alla protezione dei dati personali che lo riguardano"*
- Elevazione a diritto fondamentale dell'individuo della tutela del bene dato personale
- Principio di necessità e non eccedenza

Figure Coinvolte nel Trattamento dei Dati

- Titolare del Trattamento Dati
- Responsabile del trattamento Dati
- Incaricato del Trattamento Dati
- Interessato del trattamento Dati
- *Amministratore di Sistema*
- *Incaricato alla Tutela delle Password*
- *Responsabile della sicurezza*

Titolare del Trattamento

- La persona fisica o giuridica che ha la responsabilità finale e assume le decisioni fondamentali afferenti al trattamento dei dati
- Ove il titolare sia una persona giuridica, l'azienda stessa assume questa qualifica

Responsabile del Trattamento

- Persona fisica o giuridica, o ente, dotata di particolari caratteristiche di natura morale e di competenza tecnica
- Anche senza essere dotata di titoli di studio o esperienze formalizzate, deve comunque essere in grado di garantire al trattamento dei dati uno svolgimento fluido, corretto e soprattutto sicuro
- Ove necessario per esigenze organizzative, possono essere designati più responsabili
- I compiti affidati al responsabile devono essere analiticamente specificati per iscritto

Incaricato del Trattamento

- Persona fisica che materialmente provvede nel quotidiano al trattamento dei dati, secondo le istruzioni del titolare e/o del responsabile

Interessato del Trattamento

- Persona fisica, giuridica, l'ente o l'associazione cui si riferiscono i dati personali
- E' l'attore principale per il quale nasce Il Codice privacy in quanto "unico sovrano" dei dati personali che lo riguardano

Amministratore di Sistema

- Persona fisica o giuridica che ha il compito di governare e controllare il sistema informatico
- Non tocca quindi all'amministratore di sistema decidere i profili di accesso ai dati, amministrare la sicurezza fisica del sistema informativo
- Per la delicatezza dell'incarico, sarebbe opportuno designare l'amministratore di sistema per iscritto come un responsabile

Il Preposto alla Tutela delle *Password*

- Un soggetto con particolari competenze, a cui viene affidato il compito di conservare, in condizioni di sicurezza, le *password* degli incaricati
- Per la delicatezza dell'incarico, il "preposto" deve essere designato per iscritto
- Il ruolo può essere rivestito anche dal titolare, da un responsabile o dall'amministratore di sistema
- Il "preposto" dovrebbe vigilare sul corretto impiego delle *password* da parte degli utenti

Raccolta e Requisiti dei Dati: le Modalità

Trattamento e conservazione secondo

- Liceità e correttezza
- Pertinenza e completezza e non eccedenza rispetto alle finalità di raccolta
- Il tempo necessario per il conseguimento dello scopo

Raccolta e Requisiti dei Dati: l'Informativa

- Rappresenta una comunicazione all'interessato
- Deve essere antecedente alla raccolta
- Può essere scritta od orale
- Deve contenere
  - Finalità e modalità del trattamento
  - Natura obbligatoria o facoltativa del conferimento
  - Conseguenze di un eventuale rifiuto del consenso
  - Ambito di comunicazione e diffusione dei dati
  - Diritti dell'interessato
  - Nominativo del titolare e del responsabile

I Diritti dell'Interessato: il Consenso

- Rappresenta una comunicazione di assenso che legittima il titolare al trattamento dei dati
- Può essere totale o parziale
- Deve essere documentato per iscritto
- Deve essere un consenso informato
- Non è richiesto
  - Se il trattamento deriva da obbligo di legge
  - Se il dato è pubblico
  - Se è necessario per l'adempimento di un obbligo contrattuale

I Diritti dell'Interessato: (artt. da 7 a 10)

- Conoscenza ed accesso ai dati che lo riguardano
- Richiesta di cancellazione, trasformazione in forma anonima o blocco dei dati trattati in violazione di legge
- Richiesta di aggiornamento ed integrazione dei dati
- Opposizione totale o parziale al trattamento dei dati per motivi legittimi nonché per finalità di informazione commerciale o pubblicitaria
- Possibilità di conferire delega scritta a persone fisiche o associazioni

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

I Dati Particolari

- **I dati sensibili**: sono quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche l'adesione a partiti e sindacati, lo stato di salute e la vita sessuale. Il trattamento di tali dati può avvenire **solo** con il consenso scritto dell'interessato
- I dati giudiziari: sono quelli idonei a rivelare provvedimenti di carattere penale.

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Le Sanzioni e i Profili di Responsabilità

- Responsabilità civile: l'inversione dell'onere della prova e risarcimento dei danni
- Responsabilità penale:
  - Omessa o infedele notificazione
  - Trattamento illecito dei dati
  - Omessa adozione delle misure minime per la sicurezza dei dati
  - Inosservanza dei provvedimenti del Garante

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Sanzioni Penali

- **Trattamento illecito**: da 6 a 18 mesi di reclusione, che possono diventare 24, per l'abusiva diffusione o comunicazione. Da 1 a 3 anni se l'illecito è per trarne profitto o cagionare un danno.
- **Falsità nelle Dichiarazioni o nella Notifica**: da 6 a 36 mesi di reclusione.
- **Omissione delle Misure Minime**: arresto sino a 2 anni e ammenda da 20.000 a 100.000 euro.
- **Mancato rispetto dei provvedimenti del Garante**: reclusione da 3 a 24 mesi.

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Sanzioni Amministrative

- **Omessa o inidonea informativa**: pagamento di una somma che varia da 6.000 a 36.000 euro, che umenta notevolmente se riguarda dati sensibili.
- **Irregolarità nella cessione dei dati**: pagamento di una somma che varia da 10.000 a 60.000 euro.
- **Omessa o difforme Notificazione al Garante**: pagamento di una somma che varia da 20.000 a 120.000 euro
- **Omessa informazione o esibizione di documenti al Garante su sua richiesta**: da 8.000 a 48.000 euro.

Reattività del Sistema Rispetto alle Sollecitazioni Esterne

- Richiesta di accesso
- Richiesta risarcimento danni

Allegato B "Misure minime di sicurezza"

- Trattamento con l'ausilio di strumenti elettronici
- Trattamento senza l'ausilio di strumenti elettronici

Trattamento dei Dati con strumenti automatizzati

	Trattamento di dati personali "comuni"	Trattamento di dati sensibili o giudiziari	Trattamento di particolari dati sensibili da organismi sanitari
Autenticazione (punti 1 e 2)	**UserID + password** Dispositivo di autenticazione + password o userID Caratteristica biometrica + password o user ID		
Procedure per il corretto impiego delle credenziali (punti 3, 4 e 6)	Le credenziali sono **proprie di ogni incaricato**, anche in tempi diversi. Un incaricato può avere più credenziali per trattamenti diversi Le credenziali vanno tenute **segrete** e conservate con **diligenza**		
Requisiti di complessità delle password (Punto 5)	Password lunga almeno **8 caratteri** **Non riconducibile** all'utente Modificata al primo utilizzo ed ogni **6 mesi**	Password lunga almeno **8 caratteri** **Non riconducibile** all'utente Modificata al primo utilizzo ed ogni **3 mesi**	
Disattivazione delle credenziali (punti 7 e 8)	Non utilizzate da almeno 6 mesi Se l'utente perde le qualità di incaricato		

Trattamento dei Dati con strumenti automatizzati

	Trattamento di dati personali "comuni"	Trattamento di dati sensibili o giudiziari	Trattamento di particolari dati sensibili da organismi sanitari
Punto 9	Lo strumento elettronico non deve essere lasciato: Incustodito Accessibile		
Procedure per il garantire l'accesso ai dati e agli strumenti (punto 10)	Disporre istruzioni scritte per garantire la disponibilità di dati e strumenti Nomina di un **preposto** alla tutela delle copie delle password. Le copie sono utilizzabili solo in caso di prolungata assenza dell'incaricato e reale necessità operativa o per la sicurezza.		
Autorizzazione (punto 12)	Si richiede l'impiego di autorizzazione informatica quando sono individuati profili di incarico diversi.		
Profili di autorizzazione (punti 13, 14, 15)	**Individuali** o per **gruppi** Configurati **anteriormente** all'inizio del trattamento Verificati almeno ogni **anno** Lo stesso vale anche per gli *accaunt* **amministrativi**		

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Trattamento dei Dati con strumenti automatizzati

	Trattamento di dati personali "comuni"	Trattamento di dati sensibili o giudiziari	Trattamento di particolari dati sensibili da organismi sanitari
Virus e rischio di intrusione "*da programmi malefici*" (punto 16)	Impiego di **antivirus** *(ma anche di firewall si pensi ai worm come Blaster)* Aggiornamenti ogni **6 mesi** (palesemente inadeguato)		
Aggiornamento dei programmi (punto 17)	Aggiornamenti **annuali**, per prevenire le vulnerabilità	Aggiornamenti **semestrali**, per prevenire le vulnerabilità	
Copie di sicurezza e ripristino (punto 18) (punti 21, 22, 23)	Frequenza **settimanale** (palesemente inadeguato) Impartire istruzioni tecniche ed organizzative per le copie	Frequenza **settimanale** (palesemente inadeguato) Impartire istruzioni tecniche ed organizzative per le copie **Inintelligibiltà** dei supporti prima del riutilizzo o **distruzione** Istruzioni per la **custodia** dei supporti Ripristino dei dati in max **7 giorni**	
Accesso abusivo (punto 20)		**Firewall o IDS**	

Studio Reginelli 28

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N. **Studio Reginelli 29**

Trattamento dei Dati con strumenti automatizzati

	Trattamento di dati personali "comuni"	Trattamento di dati sensibili o giudiziari	Trattamento di particolari dati sensibili da organismi sanitari
Dati sulla salute o sessualità (punto 24)			Trattamento **disgiunto** dagli altri dati personali (es. ulteriore password) o la crittografia
Dati genetici (punto 24)			In **locali protetti** accessibili ai soli incaricati Trasportati in contenitori muniti di **serratura** o equipollenti **Cifrati** se trasferiti in formato elettronico
DPS (punto 19)		Elenco Trattamenti Mansionario Analisi dei rischi Sicurezza dei locali, integrità, disponibilità Modalità di ripristino Formazione Trattamenti all'esterno	Elenco Trattamenti Mansionario Analisi dei rischi Sicurezza dei locali, integrità, disponibilità Modalità di ripristino Formazione Trattamenti all'esterno **Cifratura e disgiunzione**
Tutela e garanzia (punti 25, 26)	Attestazione di conformità al disciplinare tecnico delle misure implementate da soggetti esterni Riferimenti al DPS nella relazione accompagnatoria del bilancio di esercizio		

AZIENDA OSPEDALIERA UNIVERSITARIA –S.U.N.

Trattamento dei Dati con strumenti <u>non</u> automatizzati

	Trattamento di dati personali "comuni"	Trattamento di dati sensibili o giudiziari	Trattamento di particolari dati sensibili da organismi sanitari
"Mansionario" (punto 27)	**Lista incaricati**, anche per gruppi omogenei Aggiornamento **annuale** della lista **Istruzioni scritte** per tutto il ciclo di trattamento, indicando i tipi di dati che possono trattare		
Controllo dei documenti (punto 28)		I documenti fuori dagli archivi devono essere sempre sotto il **diretto controllo** dell'incaricato	
Accesso agli archivi (punto 29)		Archivi ad **accesso controllato** (Presidio umano o strumenti elettronici) Dopo l'orario di chiusura **identificare e registrare** chi accede In caso in cui non esista controllo, gli accessi devono essere **autorizzati** in anticipo	

Studio Reginelli 30