© Foto di Stefano Benassi

Privacy e Sicurezza delle Informazioni

Dott.ssa Manuela Zecca

Formazione

- **Definizioni**
- **Casi di studio**
- **Adeguamento organizzativo**
  (definizione ruoli interni/esterni)
- **Rapporti con gli interessati**
  (garantire il diritto alla privacy)
- **Rapporti con il Garante**
  (notifica/autorizzazioni dati sensibili/provvedimenti)
- **Revisione dei processi**
  (misure di sicurezza, regolamenti/istruzioni/policy)

Cosa è la Privacy?

© Foto di Stefano Benassi

Riservatezza e privacy

Da "*riservatezza*" intesa come "*right to be left alone*"

A "*privacy*" *come informazione - controllo - protezione*

Cosa è la privacy?

- **Sovranità della persona sui propri dati personali**
- **Potere della persona di decidere in merito alle proprie informazioni**
  - ✓ A chi fornirne
  - ✓ Quando
  - ✓ Quali
  - ✓ Per farne cosa
- **Diritto alla protezione della propria intimità (e alla "non intimità")**
- **Diritto di non essere valutato da informazioni decontestualizzate**

Il diritto alla protezione dei dati personali

Art. 1. Diritto alla protezione dei dati personali

1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Art. 2. Finalità

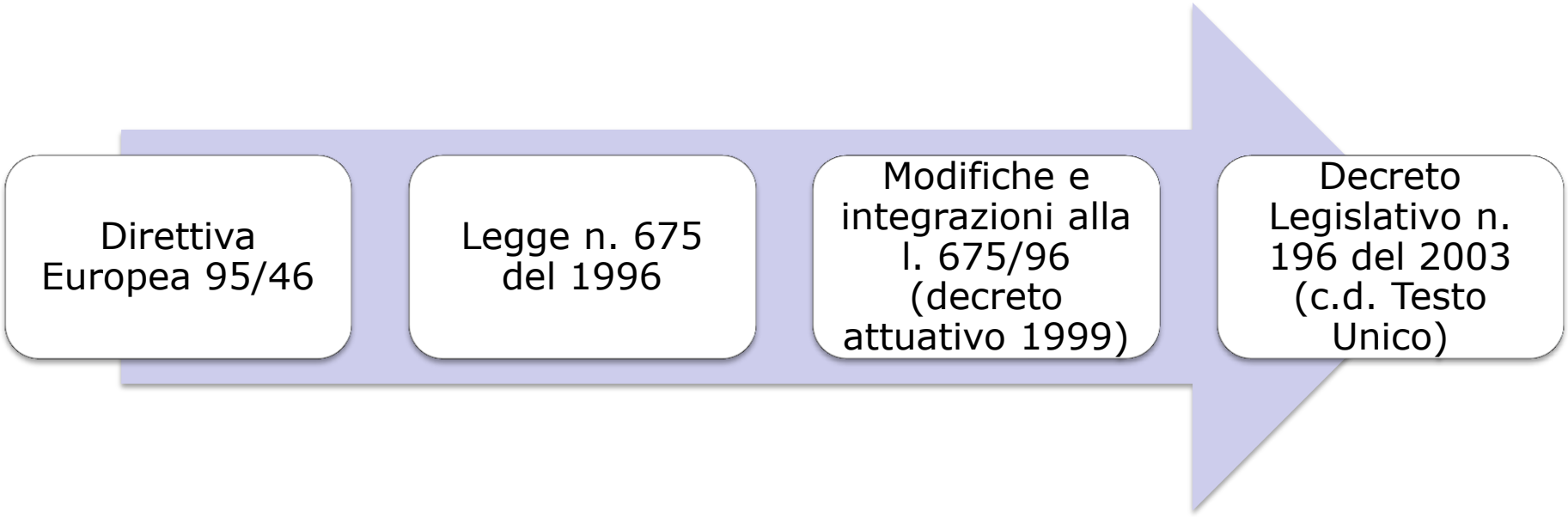
1. Il presente testo unico […] garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Dalla commissione europea: privacy come…

…"Il diritto ad essere dimenticati"

Inteso come il diritto per il cittadino di pretendere la cancellazione di qualunque dato personale archiviato su siti web (salvo sussistenza di "motivi legittimi")

Origini


Direttiva Europea 95/46
Legge n. 675 del 1996
Modifiche e integrazioni alla l. 675/96 (decreto attuativo 1999)
Decreto Legislativo n. 196 del 2003 (c.d. Testo Unico)

Codice Privacy – D.Lgs. 196/03

- **D.Lgs. 196/03**
- **Data di entrata in vigore: 01/01/2004**
- **Sostituire la vecchia legge 675/96**

Dati personali: categorie

Modulo Privacy e Sicurezza delle Informazioni

Dott.ssa Manuela Zecca

Dato personale

“Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale” (art. 4, 1, b)

413960

Dato personale: principali categorie (1/2)

Dati sensibili

Dati personali idonei a rivelare:

- origine razziale ed etnica
- convinzioni religiose, filosofiche o altro genere
- opinioni politiche
- adesione a partiti e sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- dati personali idonei a rivelare stato di salute e vita sessuale

Dato personale: principali categorie (2/2)

Dati giudiziari

Dati personali idonei a rivelare:

- 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

Livello di protezione

Trattamento (art. 4 d.lgs. 196/03)

“ 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 ”

Norme Enti Pubblici su trattamento dati comuni

Per i dati comuni, tutte le operazioni di trattamento, alla luce di quanto disposto dagli artt. 18 e 19, sono consentite soltanto nell'ambito delle funzioni istituzionali (anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente).

Nell'ambito delle stesse funzioni istituzionali, l'Ente può effettuare altre particolari operazioni di trattamento…

Caso di studio 1: “promozione evento”

La Biblioteca X del nostro Ateneo invia una comunicazione a tutti gli indirizzi e-mail degli studenti per promuovere l’evento “La seconda vita dei libri”.

Uno studente decide di agire contro la biblioteca.

Spunti di riflessione:

- *L’indirizzo e-mail dello studente è dato personale?*
- *Il trattamento dell’indirizzo e-mail da parte della biblioteca è legittimo?*

Particolari operazioni di trattamento

Art. 4 d.lgs. 196/03 co. 1

l) "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;

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

Comunicazione

Trasmissione di dati personali tra autonomi Titolari

Esempi?

Diffusione – esempi?

© Foto di Stefano Benassi

Comunicazione di dati comuni da PA a:

Alla luce di quanto disposto dall'art. 19 (Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari) del d.lgs 196/03:

- [….]
- La comunicazione da parte di un soggetto pubblico ad altri **soggetti pubblici** è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali […]
- La comunicazione da parte di un soggetto pubblico a **privati** o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Punto di attenzione

La comunicazione e la diffusione sono operazioni soggette a specifici vincoli!

Norme per gli Enti Pubblici

Alla luce di quanto disposto dall'art. 20 (Principi applicabili al trattamento di dati sensibili)

- Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati […] e di operazioni eseguibili e le finalità […] perseguite.
- Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività […] che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato […].

Alla luce di quanto disposto dall'art. 21 (Principi applicabili al trattamento di dati giudiziari)

- Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante […]

Regolamento dati sensibili e giudiziari

Schema tipo di regolamento sul trattamento dei dati sensibili e giudiziari predisposto dalla CRUI-Università in conformità al parere espresso dal Garante per la protezione dei dati personali, ai sensi dell'art. 154, comma 1, lett. g), del D.lgs. 30 giugno 2003, n. 196, in data 14 dicembre 2005.

DECRETO RETTORALE N. 271/2009 DEL 23.02.2009
TESTO UNICO SULLA PRIVACY E
SULL'UTILIZZO DEI SISTEMI INFORMATICI

Caso di studio 2: "evento di un soggetto terzo"

La Biblioteca X di un Ateneo molisano chiede ad una biblioteca dell'Ateneo di Bologna di avere tutti gli indirizzi e-mail degli studenti di origine molisana per promuovere l'evento "La seconda vita dei libri". L'elenco viene fornito.

Uno studente decide di agire contro la biblioteca.

Spunti di riflessione:

- *L'Ateneo di Bologna ha agito correttamente?*

Conseguenze operative

- **Adeguamento organizzativo**
  (definizione ruoli interni/esterni)
- **Rapporti con gli interessati**
  (garantire il diritto alla privacy)
- **Rapporti con il Garante**
  (notifica/autorizzazioni dati sensibili/provvedimenti)
- **Revisione dei processi**
  (misure di sicurezza, regolamenti/istruzioni/policy)

I ruoli del Codice

Titolare dei dati personali

(l'entità nel suo complesso)

Responsabile dei dati

Incaricato al trattamento dei dati

(Chiunque tratti dei dati personali)

Responsabile del trattamento

Ai sensi del *D.lgs. 196/03, art. 29, co. 5*:

- Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare
- Vigila, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni in materia di trattamento -ivi compreso il profilo relativo alla sicurezza-;
- Vigila sull'attuazione delle proprie istruzioni

Esternalizzazione attività

Necessaria individuazione delle responsabilità!

Se RESPONSABILE ESTERNO

- ✓ Nomina scritta
- ✓ Clausole contrattuali "ad hoc"
- ✓ Responsabilità correlate all'attività esternalizzata
- ✓ Compiti assegnati: incluse misure minime di sicurezza
- ✓ E' necessario conservare, direttamente e specificamente, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema

Designazione Incaricati

© Foto di Stefano Benassi

- **A cura del Responsabile (o del Titolare)**
- **Tutti coloro che trattano dati personali**
- **Persona fisica (non persona giuridica)**

- **Designazione scritta (anche con preposizione ad unità organizzativa) e istruzioni scritte**

Designazione Amministratori di Sistema

- **Designazione degli amministratori di sistema**
  - è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Caso di studio 3: "Responsabilità su SOL"

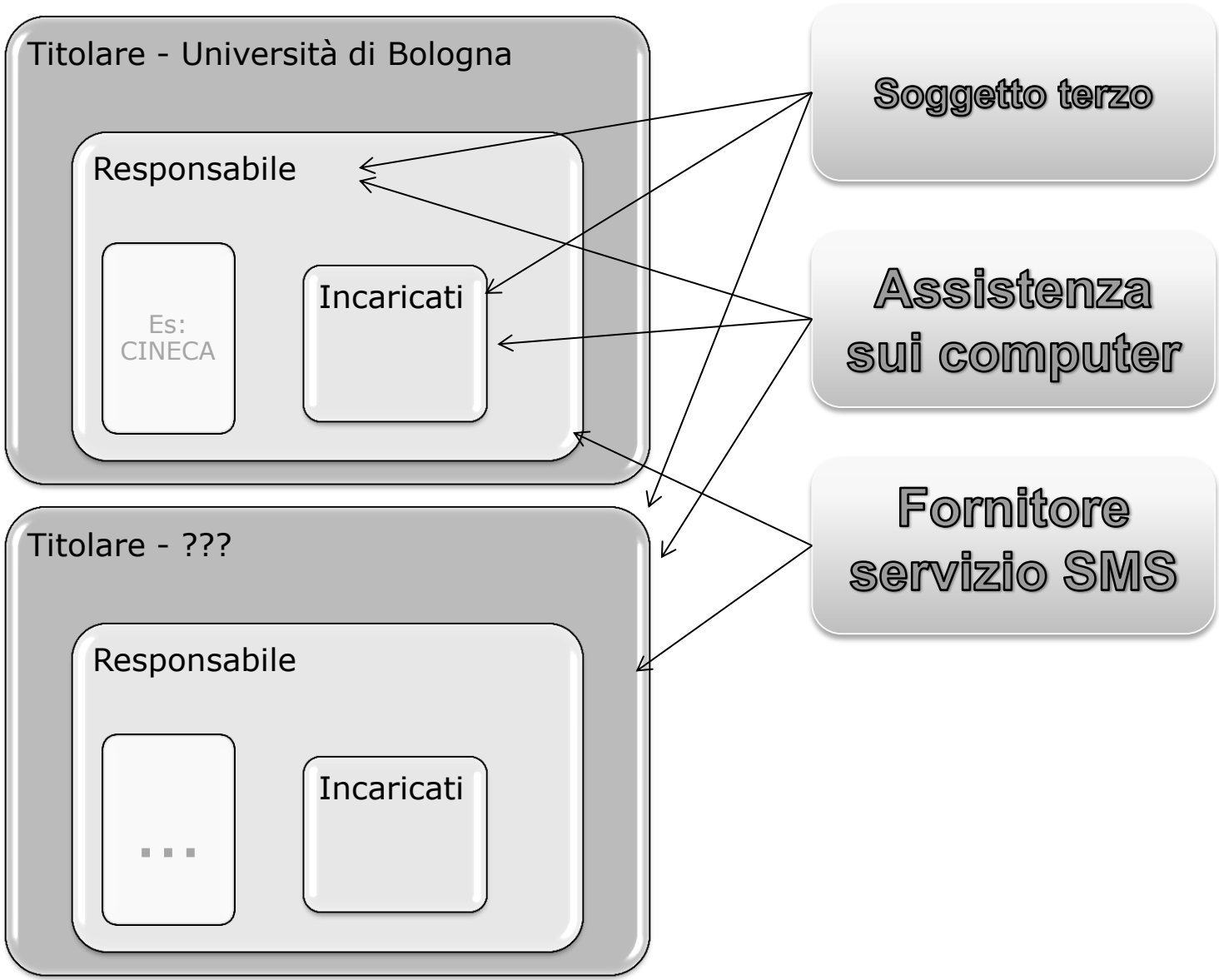
Il fornitore dell'applicativo SOL decide di inviare a tutti gli utenti presenti in SOL la propria brochure all'indirizzo di residenza segnalato nell'applicativo.

Uno dei destinatari della brochure decide di agire contro la biblioteca.

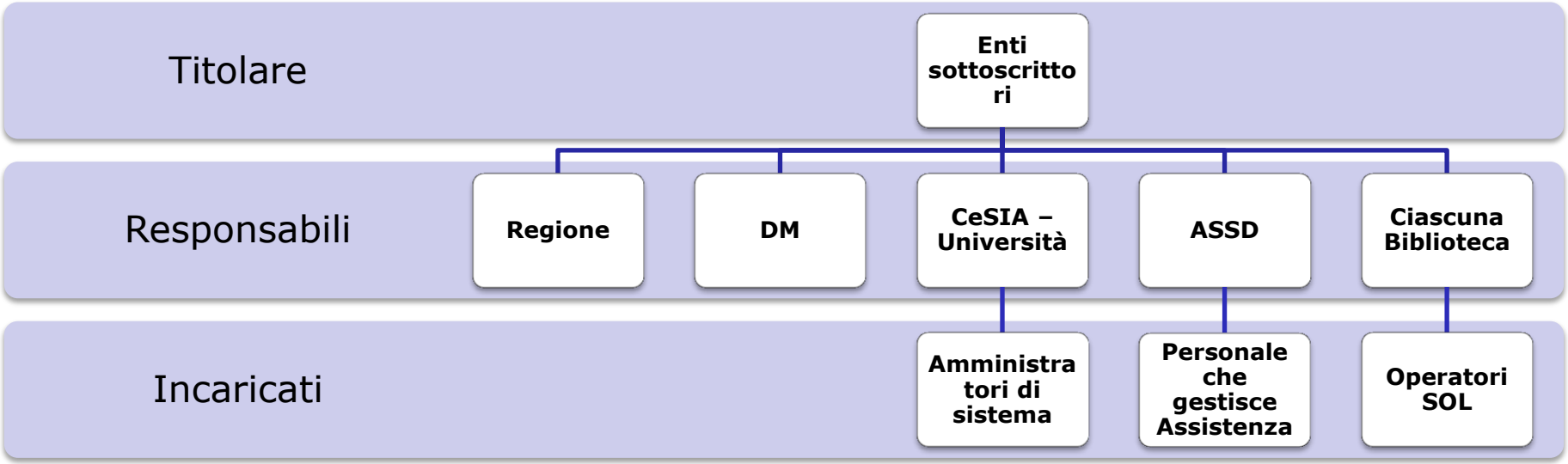
Spunti di riflessione:

- *L'indirizzo di residenza è un dato personale?*
- *Il trattamento dell'indirizzo da parte del fornitore è legittimo?*
- *Chi dovrà rispondere in giudizio?*

Dati trattati da soggetti terzi



Responsabilità SOL



Disciplinare – punto 10

Ciascuna biblioteca è Responsabile del trattamento dei dati effettuato all'interno delle proprie sedi. A titolo esemplificativo e non esaustivo, è altresì Responsabile:

- dell'esposizione dell'informativa;
- della corretta e adeguata designazione degli incaricati al trattamento dei dati personali, della loro formazione e delle istruzioni ad essi fornite;
- del mancato adeguamento delle postazioni di lavoro alle misure minime di sicurezza previste dal D.lgs. 196 del 30 giugno 2003;
- dell'eventuale designazione di un incaricato gestore delle password;
- della correttezza dei dati che sono conferiti dall'interessato;
- dell'attuazione delle istruzioni operative concordate dagli enti;
- di eventuali elaborazioni fatte dagli incaricati per fini statistici, a meno del caso in cui la biblioteca ponga in essere successivamente un'attività di comunicazione o diffusione di dati personali o di dati non sufficientemente anonimi.

Disciplinare – punto 6

I dati personali trattati nel sistema informativo condiviso possono essere oggetto di comunicazione (art. 4 co. 1 lettera l) del d.lgs. 196/03) a ciascuno dei soggetti sottoscrittori o ai soggetti aderenti esclusivamente nell'ambito delle attività svolte da tali soggetti per la gestione dei servizi bibliotecari erogati.

Se nell'ambito di tali attività di comunicazione, il soggetto sottoscrittore o l'unità organizzativa che riceve i dati dovesse utilizzarli per servizi che non sono di interesse per gli altri soggetti sottoscrittori, i dati saranno trattati sotto la propria titolarità autonoma e distinta e gli altri enti non saranno per alcuna ragione ritenuti responsabili di eventuali attività svolte nell'ambito di tali servizi. Per tale ragione, tale soggetto dovrà fornire adeguata informativa agli interessati in merito al trattamento dei dati che utilizzerà e rendere nota preventivamente a polosbnubo@unibo.it l'attività di comunicazione che intende compiere.

Conseguenze operative

- **Adeguamento organizzativo**
  (definizione ruoli interni/esterni)
- **Rapporti con gli interessati**
  (garantire il diritto alla privacy)
- **Rapporti con il Garante**
  (notifica/autorizzazioni dati sensibili/provvedimenti)
- **Revisione dei processi**
  (misure di sicurezza, regolamenti/istruzioni/policy)

Diritti dell'interessato

Informativa

Consenso

Accesso ai dati

Diritti dell'interessato

Informativa

Consenso

Accesso ai dati

Informativa

SCOPO: **DICHIARAZIONE PER METTERE IN GRADO L'INTERESSATO DI CONOSCERE LE FINALITA' DEL TRATTAMENTO, CONSENTIRGLI DI VALUTARE LE CONSEGUENZE E POTER ACCETTARE O RIFIUTARE IL TRATTAMENTO PROPOSTO**

CONTENUTO: **SCHEMA PRESTABILITO DALLA LEGGE (art. 13 del Codice)**

Contenuto dell'informativa

L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Affissione informativa

Gli addetti di tutte le sedi degli enti sono tenuti a:

A. accertarsi che l'interessato che conferisce dei dati personali transiti davanti al banco di accoglienza;

B. indicare l'informativa affissa presso il banco a chiunque venga richiesto di esibire un documento di riconoscimento o di effettuare la registrazione dei suoi dati personali;

C. non produrre in nessun caso fotocopia dei documenti di riconoscimento esibiti.

Ricordate?

L'Autorità Garante blocca l'uso dei dati per il servizio de "Le lene" - 11 ottobre 2006

SCHEDA

Doc-Web:
1345564

Data:
10/10/06

Argomenti:
Dati sanitari , Giornalismo

Tipologia:
Comunicato stampa

DOCUMENTI CITATI

Informazione televisiva e raccolta di dati genetici dei parlamentari: blocco 10 ottobre 2006 [1345622]

Stampa PDF Invia per mail

[v. Prow.ti **10 ottobre 2006** e **14 dicembre 2006**]

L'Autorità Garante blocca l'uso dei dati per il servizio de *"Le lene"*

Raccolta illecita di dati di natura sensibile in quanto attinenti allo stato di salute. Con questa motivazione l'Autorità garante per la protezione di dati personali ha disposto il blocco dell'uso dei dati personali sulla base dei quali è stato realizzato il servizio riguardante il test sull'uso di droghe effettuato, all'insaputa degli interessati, su 50 parlamentari, previsto nella puntata di stasera della trasmissione "Le lene" di Italia 1.

Il **provvedimento** cautelativo dispone, con effetto immediato, "il blocco dell'ulteriore trattamento, in qualunque forma, di ogni dato di natura personale raccolto e trattato nel caso in esame, consistente in informazioni, immagini e risultanze di *test*".

Il Garante ha rilevato, anche sulla base di quanto dichiarato dai responsabili della trasmissione riguardo alle modalità messe in atto per il *test*, che risultano al momento essere stati effettuati comunque trattamenti illeciti di dati sanitari.

L'Autorità ha infatti osservato che le norme sulla privacy risultano violate a prescindere dalla diffusione dei dati attraverso il programma televisivo, poiché una tale grave violazione dei diritti degli interessati si concretizza già al momento della raccolta dei dati.

Nel **provvedimento**, inoltre, l'Autorità sottolinea che, in particolare per chi svolge l'attività giornalistica, risulta allo stato violato il dovere di trattare i dati per scopi espliciti, di rendere note le proprie identità e lo scopo della raccolta dei dati, e di evitare artifici e comportamenti scorretti.

Roma, 10 ottobre 2006

Modalità del trattamento e requisiti dei dati

Art. 11 del D.Lgs. 196/03

1. I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Ricordate il caso di studio 1: “promozione evento”?

La Biblioteca X del nostro Ateneo invia una comunicazione a tutti gli indirizzi e-mail degli studenti per promuovere l’evento “La seconda vita dei libri”.

Uno studente decide di agire contro la biblioteca.

Diritti dell'interessato

Informativa

Consenso

Accesso ai dati

Consenso

SCOPO: **RISPOSTA (ACCETTAZIONE O RIFIUTO) DELL'INTERESSATO ALLE RICHIESTE CONTENUTE DELL'INFORMATIVA**

MODALITA':
LIBERO
INFORMATO
ESPLICITO
TOTALE O PARZIALE
DOCUMENTATO PER ISCRITTO

ESENZIONI: **LIMITATE IPOTESI PREVISTE DAL CODICE**

Consenso

I soggetti pubblici non sono tenuti a richiedere il consenso dell'interessato

Attenzione: nell'ordinamento giuridico italiano è obbligatorio il consenso al trattamento dei dati sanitari, salvo eccezioni..

Un altro caso

Bloccati dal Garante per trattamento illecito di dati personali alcuni risultati di una ricerca universitaria [...]. Gli alunni, e di conseguenza i genitori, non erano stati informati né degli scopi dell'iniziativa, né del fatto che la loro partecipazione era facoltativa e non obbligatoria.

Il provvedimento […] riguarda le informazioni personali, in alcuni casi anche sensibili, raccolte tramite questionari sottoposti ad alcuni alunni delle elementari o elaborate nelle varie fasi della ricerca, con esclusione dei dati aggregati e anonimi. A seguito del provvedimento l'Università, titolare della ricerca, non ha potuto utilizzare più queste informazioni dovendo limitarsi alla sola conservazione.[…]

Procedura illegittima e possibile violazione della privacy secondo i genitori dell'alunno, i quali si sono correttamente rivolti all'Università, lamentando anzitutto di non essere stati informati della ricerca e di non aver manifestato il loro consenso alla partecipazione, chiedendo poi di accedere ai dati personali contenuti nei questionari compilati dal figlio e opponendosi infine al loro ulteriore trattamento. Insoddisfatti della risposta ricevuta hanno presentato ricorso al Garante. […] Il Garante ha invece ritenuto illecito il trattamento dei dati personali e, a tutela dei soggetti coinvolti, ne ha disposto il blocco. Per poter svolgere legittimamente la rilevazione, infatti, l'università, operando per finalità di ricerca, avrebbe dovuto informare correttamente i genitori degli scopi dell'iniziativa e del fatto che la partecipazione dei bambini era non obbligatoria, ma volontaria. L'università ha quindi posto in essere un trattamento illecito di dati personali e per questo motivo le informazioni raccolte non sono utilizzabili.

Diritti dell'interessato

Informativa

Consenso

Accesso ai dati

Accesso ai dati

Art. 7. Diritto di accesso ai dati personali ed altri diritti

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

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

Accesso ai dati: soggetti interessati

Possono richiedere accesso ai dati…

- L’interessato
- Persone fisiche, enti, associazioni od organismi ai quali l'interessato può conferire, per iscritto, delega o procura
- Chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione nel caso di esercizio dei diritti di cui all'articolo 7 concernenti delle persone decedute

Accesso ai dati

- **Richiesta senza formalità**

  …può essere rivolta al titolare o al responsabile, anche per il tramite di un incaricato

  …può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica

- **Verifica dell'identità del richiedente**

  …l'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento.

- **Riscontro idoneo e senza ritardo**

  All'istanza il titolare o il responsabile (se designato), anche per il tramite di un incaricato, deve fornire idoneo riscontro, senza ritardo

- **Ricorso al Garante o all'Autorità Giudiziaria**

Partiamo dalle nostre attività...

© Foto di Stefano Benassi

Disciplinare – punto 7

I dati personali trattati nel sistema informativo condiviso, salvo esplicita richiesta di cancellazione da parte dell'utente, saranno conservati indefinitamente per finalità storiche. Dopo dieci anni di inattività dell'utente, i dati saranno cancellati dal sistema informativo condiviso, e conservati in archivi separati.

Disciplinare – punto 17

Il Responsabile del trattamento dovrà fornire, a seguito di eventuali istanze che gli sono direttamente sottoposte, idoneo riscontro all'interessato al fine di garantire l'esercizio dei diritti di cui all'art. 7 del d.lgs. 196/03, informando preventivamente tutti gli altri enti sottoscrittori tramite l'indirizzo polosbn@unibo.it.

Caso di studio – cancellazione dati defunto

Il Sign. Rossi si rivolge alla biblioteca X affinché siano cancellati tutti i prestiti dei libri e sia cancellata l'anagrafica del figlio che è defunto.

La bibliotecaria non concede la cancellazione del dato perché ritiene che il dato sia trattato in modo lecito e debba essere conservato per fini storici.

Spunti di riflessione:

- *E' corretta la valutazione della bibliotecaria?*

Caso di studio: “La telefonata”

Lo studente Mario Rossi frequenta da tempo la biblioteca. Lo studente riportano i libri sempre entro la scadenza, così dopo una settimana di ritardo dalla scadenza del prestito, il bibliotecario decide di avvisare tramite telefono fisso lo studente. Non trovandolo in casa, avvisa sua madre della scadenza del prestito e della necessità di provvedere alla consegna.

Spunti di riflessione:

- *Il bibliotecario ha tenuto un comportamento conforme alla normativa?*

Caso di studio

Il Sign. Rossi si rivolge alla biblioteca X tramite e-mail chiedendole di rettificare l'indirizzo di residenza e il numero del cellulare.

L'operatore SOL non esegue la modifica e chiede una raccomandata con ricevuta di ritorno per la modifica dei dati.

Spunti di riflessione:

- *E' corretta la valutazione dell'operatore?*

Conseguenze operative

- **Adeguamento organizzativo**
  (definizione ruoli interni/esterni)
- **Rapporti con gli interessati**
  (garantire il diritto alla privacy)
- **Rapporti con il Garante**
  (notifica/autorizzazioni dati sensibili/provvedimenti)
- **Revisione dei processi**
  (misure di sicurezza, regolamenti/istruzioni/policy)

Compiti del Garante

- **DIFFONDERE CONOSCENZA NORMATIVA**
- **PRESCRIVERE MISURE E ACCORGIMENTI IN MERITO AL TRATTAMENTO DI DATI CHE PRESENTANO RISCHI SPECIFICI**
- **PROMUOVERE LA SOTTOSCRIZIONE DI CODICI DEONTOLOGICI**
- **BILANCIAMENTO DEGLI INTERESSI/ESPRIMERE PARERI**
- **DECIDERE RICORSI E MISURE A SEGUITO DI RECLAMI**
- **DISPORRE ISPEZIONI E CONTROLLI**
- **SANZIONI AMMINISTRATIVE**

Provvedimenti generali

- AUTORIZZAZIONI GENERALI DATI SENSIBILI/GIUDIZIARI
- VIDEOSORVEGLIANZA
- LINEE GUIDA PER GESTIONE RAPPORTO DI LAVORO, BIOMETRIA, USO POSTA E INTERNET

  Provv. Generali 23/11/06 – 01/03/07
- USO ETICHETTE INTELLIGENTI/RFID

  Del 09/03/2005

Conseguenze operative

- **Adeguamento organizzativo**
  (definizione ruoli interni/esterni)
- **Rapporti con gli interessati**
  (garantire il diritto alla privacy)
- **Rapporti con il Garante**
  (notifica/autorizzazioni dati sensibili/provvedimenti)
- **Revisione dei processi**
  (misure di sicurezza, regolamenti/istruzioni/policy)

Misure di sicurezza

- **Mancata adozione delle misure minime**
  - Sanzione penale
  - Risarcimento danno (art. 2050)

- **Mancata adozione misure idonee**
  - Risarcimento danno (art. 2050)

Alcune misure minime di sicurezza - autenticazione

Obbligo di legge:

- Username e password per accedere ai PC/applicazioni associate a ciascun incaricato
- Password "forte" composta da almeno otto caratteri
- Password da modificare ogni 6 mesi (3 per dati giudiziari e sensibili)
- Disattivare le credenziali quando cessa il rapporto con la struttura
- Impartire istruzioni per non lasciare incustodite le sessione di lavoro

Finalità:

Evitare accessi non consentiti ai dati

Cosa offre l'Ateneo:

DSA: il sistema di credenziali istituzionale d'Ateneo.

Accesso protetto da password

Alcune misure minime di sicurezza - autorizzazioni

Obbligo di legge:

- limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento
- periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Finalità:

Evitare trattamento di dati eccedente o non pertinente

Cosa offre l'Ateneo:

DSA: il sistema di credenziali istituzionale d'Ateneo.

Autenticazione degli operatori delle biblioteche e gestione delle autorizzazioni

L'incaricato o gli incaricati che devono operare nel SIC devono essere dotati di credenziali personali.

Il responsabile invia tramite la propria e-mail istituzionale all'indirizzo asdd-sebinaol@unibo.it la richiesta di attivazione di eventuali incaricati e i profili autorizzativi ad essi assegnati. I profili di autorizzazione di ciascun incaricato dovranno inoltre essere oggetto di verifica almeno annuale da parte del relativo Responsabile che dovrà comunicare all'indirizzo sopra citato eventuali variazioni.

La richiesta di attivazione di nuove credenziali deve contenere il nominativo dell'incaricato e l'e-mail alla quale ASDD dovrà inviare le credenziali, la cui identità è preventivamente verificata dal Responsabile stesso.

Le credenziali sono create dall'Area Sistemi Dipartimentali e Documentali e inviate tramite e-mail al Responsabile del trattamento/all'indirizzo istituzionale dell'incaricato.

A seguito dell'assegnazione delle credenziali, ciascun incaricato dovrà effettuare il cambio password al primo accesso e successivamente ogni 6 mesi.

Le credenziali degli operatori non più attivi nel sistema verranno disattivate e rese inutilizzabili da altri.

Autenticazione da parte degli interessati a SIC - Portale Servizi OPAC

Nel Sistema Informativo Condiviso, gli interessati possono compiere un accesso al sistema come lettore dell'Alma Mater Studiorum – Università di Bologna o come utente del sistema SIC.

Nel caso di utenti lettori dotati di credenziali dell'Alma Mater Studiorum – Università di Bologna Ateneo, l'accesso ai servizi avviene attraverso le credenziali istituzionali @unibo.it o @studio.unibo.it.

Nel caso di utenti del sistema SIC, gli utenti accedono ai servizi attraverso la matricola lettore, costituita da un numero progressivo assegnato al momento della registrazione presso una biblioteca.

Disciplinare – punto 16

Ciascun Responsabile del trattamento individua come utilizzare i dati gestionali inerenti l'attività lavorativa di tutti gli operatori. E' fatto divieto di utilizzare i dati per attività di controllo a distanza, salvo accordo adottato da ogni singolo Responsabile del trattamento con le diverse rappresentanze sindacali ai sensi dell'art. 4 dello Statuto dei lavoratori (L. 300/1970). In caso di appalti di servizi per la gestione della biblioteca (quali ad esempio servizi di catalogazione), l'appaltatore si impegna a specificare nel contratto le modalità di utilizzo dei dati personali riferiti al committente, e registrati dal sistema ai fini della corretta esecuzione del contratto.

Disciplinare – punto 5

"I trattamenti effettuati dagli enti sottoscrittori possono essere trattati soltanto nell'ambito delle finalità istituzionali degli enti e, comunque, con lo scopo di:

- condividere le risorse bibliotecarie per una più ampia accessibilità dei documenti all'utenza;
- condividere le anagrafiche e altre informazioni sugli utenti con lo scopo di massimizzare l'efficienza e l'efficacia dei servizi bibliotecari erogati, in aderenza ai principi della Convenzione di Polo.

I dati sono trattati dagli enti sottoscrittori secondo modalità connesse a tali scopi. E' vietato effettuare operazioni di comunicazione e/o divulgazione dei dati che sono oggetto di contitolarità al di fuori dai casi espressamente previsti e autorizzati per iscritto dagli Enti tramite il presente disciplinare."