Università degli Studi di Napoli Federico II

Codice in materia di protezione dei dati personali

Clelia Baldo
C.S.I. – Centro Servizi Informativi d'Ateneo
Rossella Maio
Direzione Amministrativa

6 maggio 2010

Il Codice della Privacy (1/2)

Il primo gennaio del 2004 è entrato in vigore il decreto legislativo n. 196 del 30 giugno 2003, recante il "*Codice in materia di protezione dei dati personali*".

Rappresenta il primo modello di codificazione organica della normativa "privacy" in Europa e tiene conto sia del quadro normativo comunitario (direttive 95/46/CE e n. 2002/58/CE) che di quello internazionale.

Il Codice della Privacy (2/2)

Il Codice

1. riordina la normativa precedente in materia di trattamento e protezione dei dati personali (raggruppando, modificando e chiarendo disposizioni già vigenti),

2. introduce nuove norme

3. fornisce una regolamentazione completa per la corretta gestione dei dati personali.

Il D.Lgs. 196/2003

Composto da:

- 186 articoli
- Codici deontologici – All. A)
  - Trattamento dei dati personali nell'esercizio dell'attività giornalistica
  - Trattamento dei dati personali per scopi storici
  - Trattamento dei dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema Statistico Nazionale
- Disciplinare tecnico – All. B)
- Tavola di corrispondenza dei riferimenti previgenti al codice in materia di protezione dei dati personali

Il D.Lgs. 196/2003 e i criteri interpretativi

E' atto avente forza di legge

Ne consegue che la normativa in esso contenuta deve essere interpretata in modo da:

- risultare coerente con i principi stabiliti dalla Carta Costituzionale;
- armonizzarsi con gli altri interessi ritenuti meritevoli di tutela dall'ordinamento legislativo vigente.

Il diritto alla protezione dei dati personali

L'**articolo 1 del Codice** sancisce il "**diritto alla protezione dei dati personali**"

Obiettivo della norma: individuare "chi" e "che cosa" è protetto.

1. "**chiunque**": qualsiasi soggetto , indipendentemente dalle sue caratteristiche o dal suo status, ha diritto alla protezione dei dati personali che lo riguardano, in un'ottica di **non discriminazione**;
2. codificazione del "**diritto alla protezione dei dati personali**" come diritto **nuovo** (diritto di ciascuno a che i propri dati personali – ove trattati da terzi – siano protetti con modalità e secondo standard definiti dalla legge) ed **autonomo rispetto agli altri diritti fondamentali della persona** ed, in particolare, rispetto al diritto alla riservatezza (diritto a precludere la divulgazione e la pubblicizzazione di notizie personali).

Il diritto alla protezione dei dati personali: una eccezione

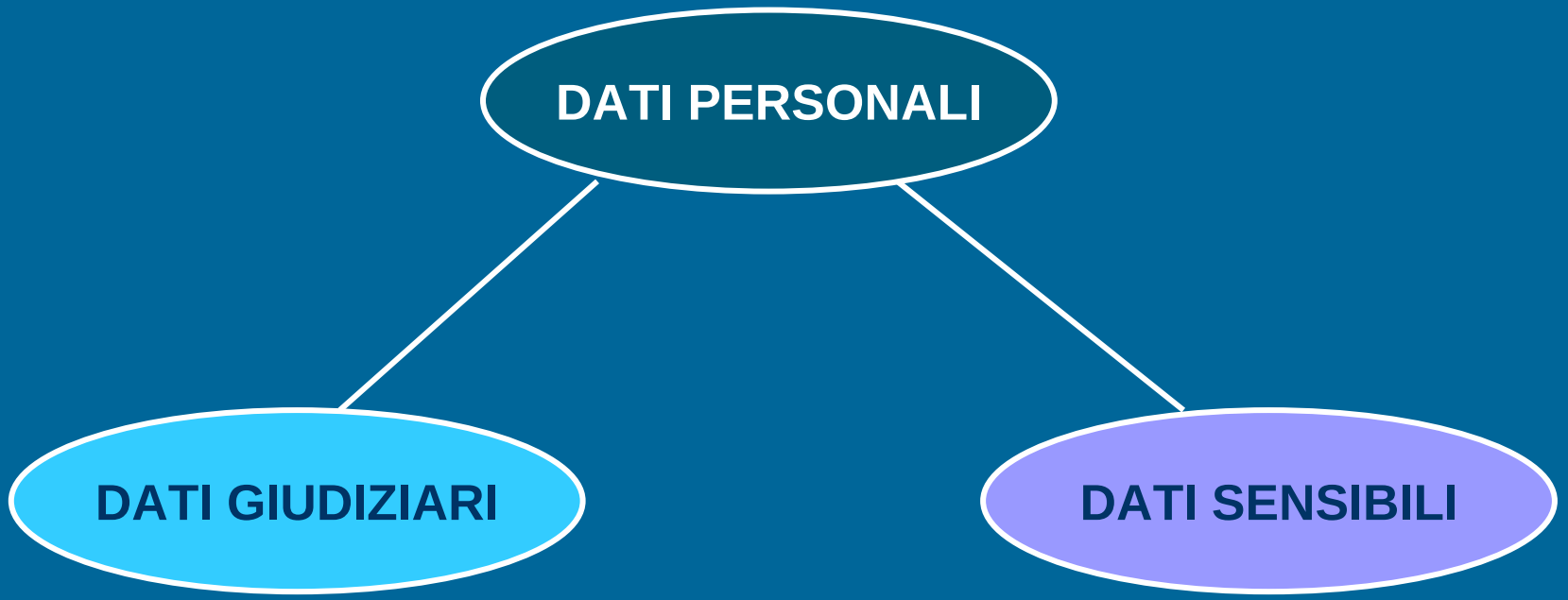
- **<u>Eccezione introdotta dall'art. 4 comma 9 della legge 15/2009</u>**: *"le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale"*

Finalità del Codice

- L'art. 2 comma 1 enuncia le **finalità del Codice**: "*garantire 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*."

- L'art. 2 comma 2 sancisce che "*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".*

I dati da proteggere



Definizioni (1/3)

dati personali: "*qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".

Un interessato è “identificabile indirettamente” quando, con l’impiego di mezzi ragionevoli e proporzionali rispetto al pericolo di lesione dei suoi diritti, è possibile stabilire un’associazione significativamente probabile tra i dati e la persona fisica, la persona giuridica, l’ente o l’associazione cui si riferiscono i dati personali.

Definizioni (2/3)

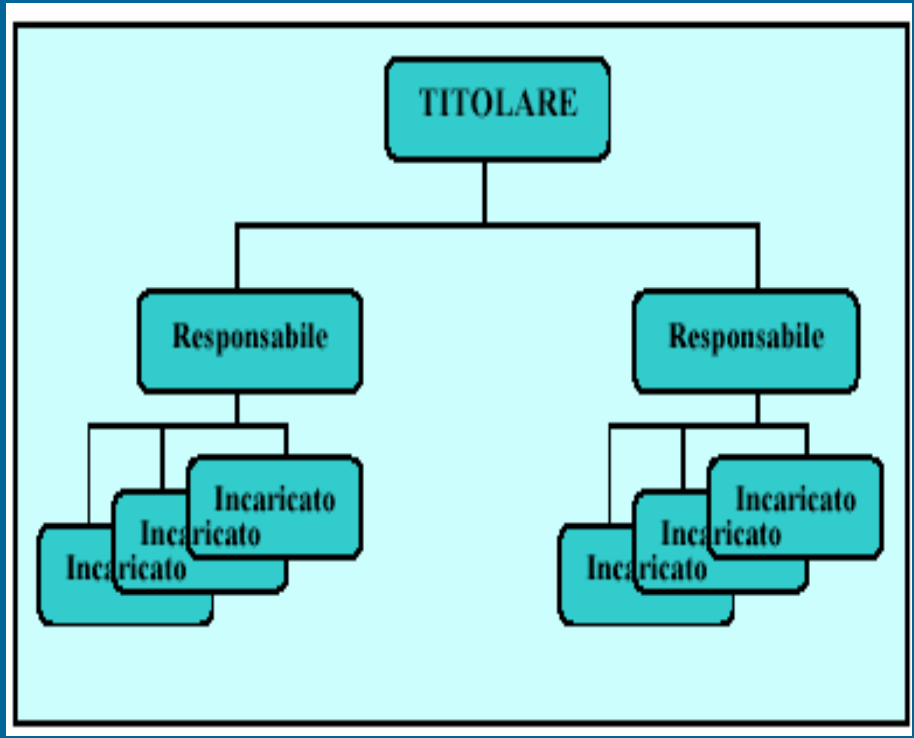
dati sensibili: sono "*i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati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

dati giudiziari*: sono quelli idonei a rivelare provvedimenti di iscrizione nel casellario giudiziale o nell'anagrafe delle sanzioni amministrative dipendenti da reato e i relativi carichi pendenti, o la qualità di imputato o di indagato.*

Definizioni (3/3)

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

I soggetti che effettuano i trattamenti (1/3)



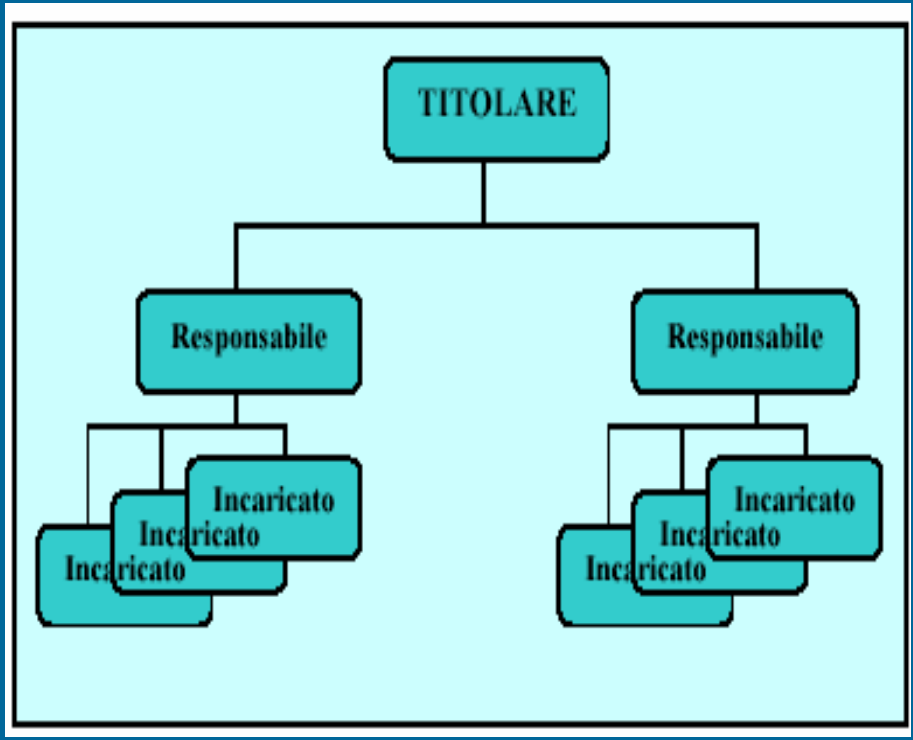
Titolare

Persona fisica, persona giuridica, pubblica amministrazione, e qualsiasi altro ente, associazione, organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, compreso il profilo della sicurezza.

I soggetti che effettuano i trattamenti (2/3)

Responsabile

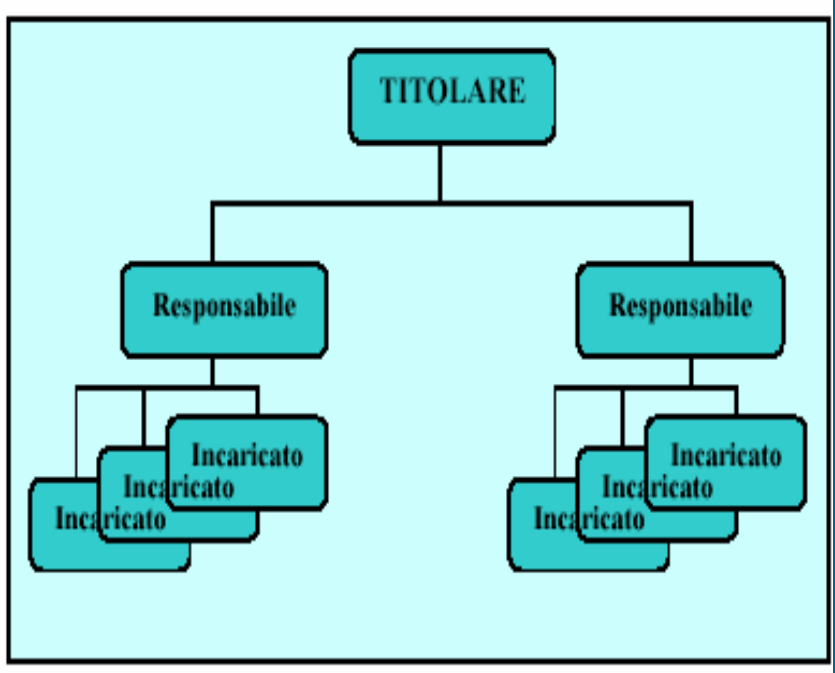
Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente o organismo preposto dal titolare al trattamento.



Inoltre,

- E' designato dal titolare
- La designazione del responsabile è facoltativa, non obbligatoria.
- Il responsabile va individuato tra i soggetti che, per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare, nel dispositivo di nomina.

I soggetti che effettuano i trattamenti (3/3)



Incaricato

Persona **fisica** autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto dal titolare o dal responsabile ed individua puntualmente l'ambito del trattamento consentito.

I principi fondamentali (1/7)

Art.3: "*I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità".*

I principi fondamentali (2/7)

L'art.3 sancisce il **Principio di minimizzazione dei dati** (ridurre al minimo l'utilizzazione di personali e di dati identificativi) che si sviluppa in due direzioni:

- **1. Principio di necessità:** il trattamento dei dati deve essere effettuato solo quando necessario, privilegiando, al massimo, l'uso di dati anonimi;
- **2. Principio di essenzialità dei dati personali utilizzati:** devono essere utilizzati soltanto i dati indispensabili per il perseguimento del fine – lecito e dichiarato – connesso al trattamento.
- **A tale fine vanno anche adeguatamente concepiti sistemi informativi e programmi informatici.**

I principi fondamentali (3/7)

Art.11, comma 1: "*I dati personali oggetto di trattamento sono:*

A. *Trattati in modo lecito e secondo correttezza;*
B. *Raccolti e registrati per scopi determinati, espliciti, 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***"**

I principi fondamentali (4/7)

L'art.11, comma 1a sancisce il Principio di liceità e correttezza del trattamento:

- il trattamento è lecito quando è conforme alle leggi, ai regolamenti, alla normativa comunitaria. Il principio di liceità implica che il titolare debba rispettare non solo la normativa contenuta nel Codice della Privacy, ma anche le specifiche discipline che possono trovare applicazione in settori particolari.
- Il trattamento è corretto quando effettuato secondo il canone di "buona fede" inteso in senso civilistico.

I principi fondamentali (5/7)

L'art.11, comma 1b sancisce il Principio di finalità del trattamento:

- il trattamento deve essere effettuato **per scopi legittimi**: sono inammissibili trattamenti con scopi illeciti o illegittimi (cioè leciti, ma non corretti);
- il trattamento deve essere effettuato **per scopi determinati**: inammissibili i trattamenti effettuati per finalità generiche, ambigue o in corso di definizione;
- Il trattamento deve essere effettuato **per scopi manifesti all'atto della raccolta dei dati** (i successivi utilizzi non possono essere incompatibili con la finalità dichiarata).

Corollari del principio di finalità sono i principi di:

- **pertinenza** : il dato trattato deve essere funzionale allo scopo perseguito:
- **completezza :** il dato trattato deve essere completo, per essere idoneo al raggiungimento dello scopo perseguito;
- **non eccedenza:** il dato trattato deve essere sufficiente per il raggiungimento dei fini, ma non eccedente i fini stessi.

I principi fondamentali (6/7)

L'art.11, comma 1c sancisce il Principio di qualità del trattamento: i dati trattati devono essere esatti, se necessario aggiornati, e completi.

Corollari del principio di qualità sono i principi di:

1. **Esattezza (o attendibilità) dei dati:** i dati trattati non devono essere erronei e non devono indurre in equivoco in relazione ad elementi di fatto. Il Titolare deve procedere a verifiche (anche periodiche) della correttezza dei dati, perché eventuali errori possono esporlo a responsabilità per danni.
2. **Aggiornamento dei dati** : solo ove necessario, atteso che ci sono dati personali "invarianti" (es.: nascita e tutti i dati con valenza storica o storicizzati).
3. **Completezza dei dati** :la completezza va valutata con riferimento alla finalità dichiarata del trattamento, perché uno stesso dato può essere valutato "completo" rispetto ad un determinato scopo e "incompleto" rispetto ad altro scopo.

I principi fondamentali (7/7)

L'art.11, comma 1d sancisce il Principio di conservazione dei dati per una periodo di tempo adeguato e non eccedente alle finalita':

I dati devono essere conservati per il tempo necessario a realizzare gli scopi del trattamento. Una conservazione eccessiva sottrae i dati al controllo dell'interessato e dello stesso titolare, aumentando i rischi di distruzione, perdita e accesso non autorizzato, oltre che i rischi di modifica illegittima dello scopo.

I diritti degli interessati (1/3)

DIRITTI DI "CONOSCENZA"

- L'interessato ha diritto di ottenere (**art. 7, comma 1**):
  la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se ancora non registrati, e la loro comunicazione in forma intelligibile.

- L'interessato ha diritto di conoscere (**art. 7, comma 2**):
  - L'origine dei dati personali
  - Le finalità e le modalità del trattamento
  - La logica applicata, in caso di trattamento effettuato con l'ausilio di strumenti elettronici
  - Gli estremi identificativi del titolare e dei responsabili
  - Le categorie di soggetti ai quali i dati possono essere comunicati

I diritti degli interessati (2/3)

DIRITTI DI INTERDIZIONE SUI DATI

- L'interessato ha diritto di ottenere (**art. 7, comma 3**):

1. l'aggiornamento, la rettificazione, ovvero, quando via ha interesse, l'integrazione dei dati che lo riguardano;
2. la cancellazione (cioè la materiale distruzione del contenuto informativo, non più ricostruibile), la trasformazione in forma anonima ed il blocco (cioè la conservazione dei dati personali con sospensione temporanea di ogni altra operazione del trattamento), se i dati sono trattati in violazione di legge;
3. l'attestazione che le operazioni di cui sopra sono state portate a conoscenza di coloro a cui i dati sono stati comunicati o diffusi, qualora tale adempimento sia possibile e non comporti "*un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato*".

I diritti degli interessati (3/3)

DIRITTI DI OPPOSIZIONE

- L'interessato ha infatti il diritto di opporsi (art. 7, comma 4):

1. per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta
2. al trattamento per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale

Esercizio dei diritti dell'interessato (1/2)

- I diritti degli interessati definiti nell'art.7 sono esercitati con richiesta:

1. rivolta al titolare o al responsabile del trattamento, **anche per tramite di un incaricato;** (la richiesta va indirizzata al Titolare o al Responsabile ed è ricevibile da un Incaricato);
2. **senza formalità** (raccomandata A/R, fax, posta elettronica, oralmente se si tratta dei diritti di cui ai commi 1 e 2 dell'art.7);
3. alla quale è fornito idoneo riscontro **senza ritardo** .

Termine per il riscontro:

1. **15 giorni** dalla ricezione della richiesta;
2. se le operazioni necessarie per un integrale riscontro sono di particolare complessità, o ricorre altro giustificato motivo, il titolare o responsabile ne danno comunicazione all'interessato. In tal caso, il termine per il riscontro è di **30 giorni**.

Esercizio dei diritti dell'interessato (2/2)

- Ammissibilità di conferimento di delega a terzi (persone fisiche, enti, associazioni, organismi) per l'esercizio dei diritti di cui all'art. 7.
- Obbligo di chi riceve la richiesta di accertare l'identità del richiedente (tramite esibizione o rilascio di copia di documento di identità, esibizione della eventuale delega o procura).
- La richiesta relativa ai diritti di trasparenza di cui ai commi 1 e 2 dell'articolo 7 (diritti di conoscenza) può essere liberamente formulata, salva l'esistenza di giustificati motivi, ad intervalli non minori di 90 giorni (art. 9, comma 5).

Riscontro all'interessato (1/2)

- **<u>Modalità del riscontro:</u>**

I dati estratti possono essere (art. 10, comma 2):

- comunicati all'interessato verbalmente;
- offerti in visione mediante strumenti elettronici
- Su richiesta dell'interessato,trasposti su supporto cartaceo o informatico o trasmessi per via telematica
- Mediante esibizione o consegna in copia di atti e documenti contenenti i dati richiesti, **quando l'estrazione dei dati è particolarmente difficoltosa.**

- **<u>Caratteristica distintiva del diritto di accesso privacy rispetto al diritto di accesso ai documenti amministrativi</u>:**
  - il diritto di accesso privacy ha per oggetto i dati personali che si riferiscono all'interessato e non i documenti che li contengono;
  - il Titolare non potrà consegnare copia o dare in visione il documento contenente i dati personali di riferimento, ma dovrà provvedere alla loro estrapolazione

Riscontro all'interessato (2/2)

- **Oggetto del riscontro**: totalità dei dati personali che riguardano l'interessato e che sono in possesso del titolare, salvo che l'interessato abbia circoscritto la richiesta ad un ambito più ristretto (art. 10 comma 3);
- **L'esercizio del diritto è, di regola, gratuito.**
- **Ipotesi in cui può essere posto a carico del richiedente un contributo spese:**
  - quando non risulta confermata l'esistenza di dati che riguardano l'interessato;
  - quando i dati figurano su supporto di cui è richiesta la riproduzione;
  - quando si determina un notevole impiego di mezzi in relazione alla complessità o entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

L’informativa (1/3)

- In base all’art.13, comma 1, l’interessato (o la persona presso la quale sono raccolti i dati) deve essere **preventivamente** informato circa:
  1. Le finalità e le modalità del trattamento;
  2. La natura obbligatoria o facoltativa del conferimento di dati:
     - se la fornitura dei dati deriva da un obbligo di legge;
     - se è strettamente strumentale all’esecuzione di un rapporto contrattuale;
     - se è funzionale all’attività del Titolare.
  3. Le conseguenze di un eventuale rifiuto di rispondere;
  4. I soggetti o le categorie cui i dati possono essere comunicati e l’ambito di diffusione degli stessi;
  5. I diritti di cui all’art. 7;
  6. Gli estremi identificativi del titolare e del responsabile (quando è identificato un responsabile per il riscontro all’interessato, è indicato tale responsabile).

L’informativa (2/3)

- L’informativa:

1. È requisito di legittimità del trattamento;
2. Può essere orale o scritta e, in ogni caso, deve essere formulata in modo tale da consentire la piena comprensione di tutti gli elementi indicati nell’art. 13.
3. Può non comprendere elementi già noti alla persona che fornisce i dati (ad es.: perché oggetto di precedente informativa)
4. Quando riguarda dati personali non raccolti presso l’interessato, ma presso terzi, deve essere data all’interessato all’atto della registrazione dei dati (cioè quando i dati acquisiti sono immessi nella banca dati) o comunque prima che siano comunicati a terzi.

L’informativa (3/3)

- Casi di esonero dall’obbligo di informativa:

1. Casi in cui il trattamento è effettuato per obbligo normativo;
2. Trattamenti svolti per indagini difensive o difesa in giudizio;
3. Casi in cui il Garante con proprio provvedimento riconosce che l’adempimento sia impossibile o eccessivamente oneroso.

L’omessa o inidonea informativa è sanzionata con la sanzione amministrativa del pagamento di una somma da 6000 a 36.000 (art. 161).

Regole per i soggetti pubblici

- Ai sensi dell'articolo 18, alle pubbliche amministrazioni è consentito il trattamento dei dati personali solo se è necessario a svolgere fini istituzionali e nel rispetto del Codice e delle leggi e di regolamenti.
- Gli enti pubblici non devono chiedere il consenso dell'interessato. Resta fermo l'obbligo di informativa.

Dati personali

- Ai sensi dell'art. 19:

1. Il trattamento dei dati personali diversi da quelli sensibili o giudiziari è consentito al soggetto pubblico, anche se non previsto da norma di legge o di regolamento che lo preveda espressamente;

2. La comunicazione ad altro soggetto pubblico è consentita solo quando prevista da norme di legge o di regolamento o quando necessaria per lo svolgimento di funzioni istituzionali (in questo caso, solo decorsi 45 giorni dalla comunicazione al Garante senza che vi sia stata diversa determinazione del Garante stesso);

3. La comunicazione a soggetti privati o enti pubblici economici e la diffusione sono consentite solo se previste da norme di legge o di regolamento.

Garanzie per i dati sensibili e giudiziari (1/5)

- Ai sensi degli artt. 20 e 21:

1. il trattamento di dati sensibili e giudiziari è consentito **solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati , le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite;**
2. qualora la disposizione di legge, pur specificando la rilevante finalità di interesse pubblico, non specifichi le categorie di dati sensibili che possono essere utilizzati né le operazioni eseguibili, il titolare deve rendere pubblici i trattamenti eseguiti mediante un **provvedimento di tipo regolamentare**, **adottato in conformità al parere espresso dal Garante anche su schemi tipo;**
3. **In assenza di previsione di legge** i titolari possono richiedere esplicita **autorizzazione da parte del Garante**, che individuerà, con proprio provvedimento, le attività di rilevante interesse pubblico e per le quali è, quindi, autorizzato il trattamento.

Garanzie per i dati sensibili e giudiziari (2/5)

- **Art.22 - Comma 2**: l'informativa di cui all'articolo 13 deve contenere espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

- **Art.22 - Comma 3**: i dati sensibili e giudiziari possono essere trattati solo per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

- **Art. 22 - Comma 4**: i dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

Garanzie per i dati sensibili e giudiziari (3/5)

Art. 22 - Comma 5:

- Verifica periodica in ordine a:
  1. Esattezza;
  2. Aggiornamento;
  3. Pertinenza;
  4. Completezza;
  5. Non eccedenza;
  6. Indispensabilità dei dati.
- Inutilizzabilità dei dati eccedenti, non pertinenti, non indispensabili
- Ammissibilità della sola conservazione dell'atto o documento che li contiene (custodia passiva, un "blocco di dato", sul quale non sono ammesse altre possibilità di trattamento).

Garanzie per i dati sensibili e giudiziari (4/5)

Art. 22 commi 6 e 7: Speciali misure di sicurezza dettate per i dati sensibili e giudiziari

- I dati sensibili e giudiziari, **se sono registrati un banca dati elettronica**, devono essere **cifrati** mediante l'utilizzo di algoritmi crittografici o di codici identificativi o di altre soluzioni che li rendono temporaneamente inintellegibili anche a chi è autorizzato ad accedervi e permettono di identificare l'interessato solo in caso di necessità.

- I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo e non possono essere diffusi. Devono essere cifrati anche se registrati in banca dati non elettronica.

Garanzie per i dati sensibili e giudiziari (5/5)

L'omissione delle misure di cui ai commi 6 e 7 per la tutela dei dati sensibili e giudiziari integra omissione di misure minime di sicurezza punito con l'arresto sino a 2 anni e la pubblicazione della sentenza (art. 169).
La violazione dell'art. 22 comma 8 (divieto di diffusione dati relativi allo stato di salute) è punito, se dal fatto deriva nocumento e se la violazione è stata effettuata al fine di trarre profitto o di arrecare danno, con la reclusione da 1 a 3 anni.

Disciplina dei dati sanitari (1/2)

- **Nel settore pubblico**, il trattamento di dati sanitari per **finalità diverse da quelle sanitaria** (ad esempio per la gestione del rapporto di lavoro, per fini assicurativi e previdenziali) **non necessita di consenso da parte dell'interessato e della preventiva autorizzazione del Garante** (art. 18 comma 4)

- **Il trattamento è soggetto alle prescrizioni generali relative ai dati sensibili (artt. 20 e 22).**

Disciplina dei dati sanitari (2/2)

Se il trattamento è effettuato da un ente pubblico per scopi sanitari:

1. nel caso di salvaguardia dell'incolumità fisica o di tutela della salute dell'interessato è richiesto il relativo consenso;

2. Nel caso di tutela dell'incolumità fisica di un terzo o della collettività, il trattamento dei dati può essere eseguito anche senza il consenso dell'interessato, previa autorizzazione del Garante (rilasciata, di norma, sentito il parere del Consiglio superiore di sanità).

La notificazione (1/3)

- **<u>Comunicazione preventiva al Garante relativa a particolari trattamenti svolti da alcuni Titolari.</u>**

- Il Codice, nell'art. 37, comma 1, individua ed elenca le categorie di trattamenti soggetti all'obbligo di notificazione.

- I dati comunicati al Garante sono inseriti in un registro elettronico, consultabile dagli interessati, anche telematicamente e gratuitamente.

La notificazione (2/3)

Tra i casi previsti dal legislatore, vanno notificati i trattamenti sui seguenti dati:

- ✓ Genetici o biometrici oppure volti a monitorare la posizione geografica di persone o cose mediante strumenti elettronici;
- ✓ Idonei a rivelare lo stato di salute e la vita sessuale, ai fini di: procreazione assistita, prestazione di servizi sanitari, indagini epidemiologiche, banche dati, rilevazioni di malattie, monitoraggio della spesa sanitaria
- ✓ Volti a definire il profilo o la personalità dell'interessato o ad analizzarne abitudini o scelte di consumo (trattati con ausilio di mezzi elettronici);
- ✓ Sensibili, registrati in banche dati ai fini di selezione del personale per conto terzi o utilizzati per sondaggi di opinione e ricerche campionarie in generale;
- ✓ Relativi al rischio della solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti e fraudolenti (registrati in banche dati gestite con strumenti elettronici).

La notificazione (3/3)

- Il Garante, con la propria deliberazione del 31.3.2004 e successivo parere del 23.4.2004, sottrae a tale obbligo alcuni trattamenti.

- A titolo di esempio, sono esclusi dalla notificazione i seguenti trattamenti:

✓ I trattamenti dei dati idonei a rivelare la sfera psichica dei lavoratori, nel caso di adempimenti di legge o di diritto al lavoro dei disabili;

✓ I trattamenti di dati personali relativi al rischio sulla solvibilità economica, purché utilizzati per adempiere esclusivamente obblighi normativi in materia, di rapporto di lavoro, previdenza o assistenza;

✓ La registrazione di immagini o suoni, di ingressi e di uscite da luoghi di lavoro, purché non abbiano il carattere del "tracciamento" continuo.

Omessa o incompleta e falsa notificazione

L’omessa o incompleta notificazione è punita con la sanzione amministrativa del pagamento di una somma da 20.000 a 120.000 euro e la pubblicazione dell’ordinanza – ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica (art.163).

La falsa notificazione (art.168) è invece perseguita penalmente, con la reclusione da sei mesi a tre anni e la pubblicazione della sentenza.

Trattamenti per scopi scientifici

- Ha una disciplina specifica (artt. 97 e ss.);
- Le finalità relative ai trattamenti effettuati per scopi scientifici da soggetti pubblici hanno “rilevante interesse pubblico” (art. 97);
- Il trattamento effettuato per scopi scientifici è considerato compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti e trattati
- Il trattamento può essere effettuato anche oltre il periodo di tempo per conseguire i diversi scopi per i quali i dati sono stati in precedenza trattati;
- Per scopi scientifici, i dati per i quali, per qualsiasi causa è cessato il trattamento, possono essere conservati o ceduti ad altro titolare;
- Per promuovere la ricerca i soggetti pubblici (comprese le università)possono comunicare e diffondere, anche a privati, dati relativi ad attività di studio e ricerca, a laureati, dottori di ricerca, docenti, esperti e studiosi, con esclusione dei dati sensibili e giudiziari (fermo il diritto dell’interessato ad opporsi al trattamento per motivi legittimi)

Videosorveglianza

- Provvedimento del Garante del 29 aprile 2004: principi e prescrizioni generali relative a tutti i sistemi di videosorveglianza;
- Obiettivo del provvedimento: bilanciare esigenze di sicurezza di luoghi e persone con libertà di circolazione nei luoghi pubblici o aperti al pubblico senza subire ingerenze derivanti da rilevazioni invadenti ed oppressive riguardanti presenze, tracce di passaggi e spostamenti;
- Obbligo di informativa agli interessati (anche mediante modello semplificato, per le aree esterne);
- Designazione per iscritto delle persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni;
- 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 richiesta dell'autorità giudiziaria o di polizia giudiziaria.

Trattamenti con rischi specifici (1/3)

Trattamenti con rischi specifici (2/3)

Trattamenti su dati diversi dai sensibili e giudiziari che presentano, per la loro natura o per la modalità del trattamento, RISCHI SPECIFICI per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato (art. 17). Vanno preventivamente verificati misure ed accorgimenti adottati, anche a seguito di interpello del titolare.

La violazione delle misure e degli accorgimenti da adottare per tali trattamenti (art. 167) comporta l'applicazione di sanzioni penali, con reclusione da 1 a 3 anni se dal fatto deriva nocumento e la pubblicazione della sentenza.

Trattamenti con rischi specifici (3/3)

- Assenza di individuazione di dettaglio delle tipologie di dati da parte del Garante.
- Si potrebbe configurare il dubbio di legittimità costituzionale, considerando l'art.17 come una "norma in bianco", sanzionata penalmente (dato che la violazione dell'art. 17 può configurare il reato di "*trattamento illecito di dati personali*", in presenza degli altri presupposti richiesti dalla norma.)
- Applicazione dell'art. 17 nei casi di cui all'art. 55, rubricato "*Particolari tecnologie*":"*il trattamento di dati personali che implica maggiori rischi di un danno per l 'interessato, con particolare riguardo a banche di dati genetici o biometrici, a tecniche basate su dati relativi all'ubicazione, a banche di dati basate su particolari tecniche di elaborazione delle informazioni e all'introduzione di particolari tecnologie, è effettuato nel rispetto delle misure e degli accorgimenti di cui all'art. 17, sulla base della preventiva comunicazione dell'art. 39*" .

Misure di Sicurezza

- **Regola generale fissata dall'art. 31 (obblighi di sicurezza)**

  I dati personali oggetto di trattamento sono custoditi e controllati in modo da ridurre al minimo, **mediante l'adozione di idonee e preventive misure di sicurezza**, i rischi di:

  1. **Distruzione e perdita dei dati**
  2. **Accesso non autorizzato** (sia fisico che informatico)
  3. **Trattamento non consentito o non conforme alle finalita' della raccolta**

Misure minime di sicurezza (1/2)

- I titolari del trattamento sono comunque tenuti ad adottare le misure minime di sicurezza, volte ad assicurare un livello minimo di protezione dei dati personali (art. 33).

- **Le misure minime sono puntualmente indicate negli artt. 34 – 35 del Codice e nell'Allegato B (Disciplinare Tecnico) del Codice.**

- Si applicano anche a quei trattamenti pubblici in materia di polizia, giustizia, difesa e sicurezza dello Stato che derogano dalla generalità delle disposizioni.

- Alla mancata osservanza delle misure di sicurezza considerate minime sono collegate sanzioni di carattere penale. (art. 169)

Misure minime di sicurezza (2/2)

"*Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'art. 33, è punito con l'arresto sino a due anni* (art. 169, comma 1) e con la pubblicazione della sentenza.

Il Garante, all'atto dell'accertamento, fissa un termine comunque non superiore a sei mesi affinché siano adottate le misure di sicurezza necessarie (regolarizzazione). L'adempimento ed il pagamento della sanzione amministrativa estinguono il reato (art. 169, comma 2).

Trattamenti con e senza l'ausilio di strumenti elettronici

- Sono consentiti solo se sono adottate delle misure minime nei modi previsti dal disciplinare tecnico contenuto nell'allegato B del Codice.
- L'adozione delle misure minime di sicurezza è precondizione di liceità del trattamento.
- Gli artt. 34 e 35 del Codice contengono, rispettivamente, l'elenco delle misure minime da adottare nel caso di trattamenti effettuati con o senza strumenti elettronici.

Le misure minime di sicurezza previste dall'art. 34

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

Le misure minime di sicurezza previste dall'art. 35

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi di accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il disciplinare tecnico in materia di misure minime di sicurezza (1/2)

- E' una fonte normativa secondaria in cui sono specificate le modalità di attuazione delle misure minime.
- L'art. 36 ne prevede l'aggiornamento attraverso un "d*ecreto del Ministro della Giustizia di concerto con il Ministro per le innovazioni e le tecnologie" .*
- Si applica sia ai trattamenti automatizzati (con strumenti elettronici) che ai trattamenti non automatizzati (archivi tradizionali).
- Gli artt. 34 e 35 individuano quali funzionalità di sicurezza debbano essere implementate.
- Il disciplinare tecnico contenuto nell'Allegato B stabilisce invece come tali funzionalità debbano essere implementate, fornendone quindi le specifiche di dettaglio.

Il disciplinare tecnico in materia di misure minime di sicurezza (2/2)

Il Disciplinare è strutturato in 7 sezioni:

1. Sistema di autenticazione informatica
2. Sistema di autorizzazione informatica
3. Altre misure di sicurezza
4. **Documento Programmatico sulla Sicurezza**
5. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
6. Misure di tutela e garanzia
7. Trattamenti senza l'ausilio di strumenti elettronici

Sistema di autenticazione informatica - Definizione

E’ un dispositivo atto a stabilire e verificare in modo univoco, anche indiretto, l’identità dichiarata da un utente che vuole accedere al sistema. L’identificazione e l’autenticazione devono essere effettuate prima di ulteriori interazioni tra il sistema e l’utente.

Sistema di autenticazione informatica

art. 34, comma 1,a) -> All.B (Regole 1 ÷ 3)

- **<u>Credenziali di autenticazione (valide per uno o più trattamenti)</u>** previste:
  1. Codice identificativo dell'incaricato, associato ad una parola chiave conosciuta solo dall'incaricato;
  2. Dispositivo di autenticazione in possesso o uso esclusivo dell'incaricato (*badge* magnetico, *smart card*, chiave USB…)
  3. caratteristica biometriche dell'interessato.

- Ad ogni incaricato sono associate una o più credenziali

Gestione delle credenziali di autenticazione (1/2)

art. 34, comma 1,b) -> All.B (Regole 4÷11)

- Bisogna adottare le necessarie cautele per assicurare la segretezza delle credenziali di autenticazione e la diligente custodia dei dispositivi.
- Parola chiave deve essere basata su **almeno otto caratteri**
- La parola chiave deve essere **modificata al primo utilizzo** e poi almeno ogni sei mesi (almeno ogni tre mesi nel trattamento di dati sensibili)
- I codici identificativi (credenziali di autenticazione) non sono utilizzabili per diversi incaricati anche in tempi successivi

Gestione delle credenziali di autenticazione (2/2)

art. 34, comma 1,b) -> All.B (Regole 4÷11)

- Sono disattivate le credenziali:
  1. inutilizzate da almeno sei mesi (escluse quelle per scopi di gestione tecnica);
  2. in caso di cessazione della qualità di "incaricato";
- Sono impartite, dal titolare o dal responsabile, se nominato, istruzioni per non lasciare incustodito il PC durante una fase del trattamento);
- se l'accesso ai dati ed agli strumenti elettronici è consentita esclusivamente attraverso l'uso di un sistema di autenticazione, devono essere impartite disposizioni scritte per individuare chiaramente le modalità con cui il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di assenza o impedimento dell'incaricato, che renda indispensabile o indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema.
- La custodia della copia delle credenziali è organizzata garantendo la relativa segretezza e individuando per iscritto gli incaricati della custodia, che dovranno informare, tempestivamente l'incaricato dell'intervento effettuato.

Il Sistema di autorizzazione

art. 34, comma 1,c) -> All.B (Regole 12÷14)

- Previsto quando sono individuati profili di autorizzazione di ambito diverso
- Profili di autorizzazione, per ciascun incaricato, sono **definiti** anteriormente all'inizio del trattamento
- Garantisce che un utente/incaricato possa espletare i soli trattamenti di sua competenza
- Verifica periodica (almeno annuale) della sussistenza delle condizioni per la conservazione dei profili di autorizzazione

Aggiornamento della lista degli incaricati

art. 34, comma 1,d) -> All.B (Regola 15)

- Con cadenza almeno annuale viene identificato l'ambito di trattamento consentito per ciascun incaricato (tra cui anche gli addetti alla gestione e / o manutenzione degli strumenti elettronici).

Protezione degli strumenti elettronici e dei dati

art. 34, comma 1,e) -> All.B (Regola 16, 17 e 20)

- I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-*quinquies* del c.p.) con aggiornamento almeno semestrale (Reg.16).

- Gli aggiornamenti periodici pei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti sono effettuati con frequenza almeno annuale e cadenza almeno semestrale per i dati sensibili e giudiziari (Reg. 17).

- Per i dati sensibili e giudiziari, in aggiunta, protezione contro l'accesso abusivo (art. 615-*ter* del c. p.) con idonei strumenti elettronici (*firewall*, dispositivi hardware e software) (Reg. 20)

Procedure per la custodia di copie di sicurezza e ripristino dei dati e dei sistemi

art. 34, comma 1,f) -> All.B (Regola 18, 21, 22, 23)

- Procedure di *backup* (e *restore…*) con frequenza almeno settimanale (Reg.18)

- Modalità di *backup:*
  - Integrale/Incrementale
  - Su nastro magnetico/su disco magnetico
  - Su supporto “non obliterabile”
  - Accorta gestione dei supporti magnetici rimovibili contenenti dati sensibili o giudiziari (Reg. 21)
  - Distruzione o rimozione dei dati sensibili o giudiziari nel caso di riuso dei supporti magnetici (Reg. 22)
  - Ripristino della disponibilità dei dati entro sette giorni nel caso di dati sensibili o giudiziari (Reg. 23)

Ulteriori misure in caso di trattamento di dati idonei a rivelare lo stato di salute

art. 34, comma 1, h) -> All.B (Regola 24)

- Particolari misure tecniche, fisiche e logiche di protezione per i dati idonei a rivelare lo stato di salute e/o la vita sessuale per gli organismi sanitari e medici (Reg. 24):
  - ricorso alla cifratura
  - separazione dagli altri dati personali che permettono di identificare direttamente gli interessati
  - particolari cautele per i dati genetici: locali protetti con controllo autorizzazione degli incaricati, trasporto dei dati su supporto magnetico in contenitori sicuri o, se in formato elettronico, previa cifratura.

Il Documento Programmatico sulla Sicurezza (DPS) – Generalità (1/2)

- Richiesta la sua aggiornata tenuta già nell'art. 34, comma 1, lettera g, del Codice per ogni trattamento con strumenti elettronici
- Descritto in dettaglio nella regola 19 del Disciplinare tecnico
- La sua redazione compete al titolare, anche attraverso un responsabile, se designato

Il Documento Programmatico sulla Sicurezza (DPS) – Generalità (2/2)

- Da redigere entro il 31 marzo di ogni anno;
- Il DPS va referenziato, a cura del Titolare, nella relazione accompagnatoria al bilancio di esercizio;
- Il DPS assume, sia pur indirettamente, la forma di un "*documento pubblico*" la cui mancata redazione, o la presenza al suo interno di informazioni non veritiere, configura un reato penale (omessa adozione di misure minime ex art. 169 del Codice)

Gli elementi del DPS (1/2)

- Censimento dei trattamenti di dati personali svolti dal titolare (Reg. 19.1)
- Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento di dati(Reg. 19.2)
- Analisi dei rischi incombenti sui dati (Reg. 19.3)
- Indicazione delle misure di garanzia per l'integrità e la disponibilità dei dati, la protezione dei locali e delle aree (Reg. 19.4)
- Descrizione dei criteri e delle modalità per il ripristino dei dati a seguito di distruzione o danneggiamento, entro sette giorni nel caso di dati sensibili e giudiziari (Reg. 19.5)

Gli elementi del DPS (2/2)

- Previsione di interventi formativi a beneficio degli incaricati (Reg. 19.6)
- Descrizione dei criteri per l'affidamento di elaborazioni dati all'esterno della struttura del titolare, in *outsourcing* (Reg. 19.7)
- Descrizione dei criteri per la cifratura o la separazione di dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali dell'interessato (Reg. 19.8)

La stesura del DPS: flusso delle attività

Trattamenti senza l'ausilio di strumenti elettronici

art. 35, comma 1 -> All.B (Regole da 27 a 29)

- Istruzioni scritte agli incaricati e rilevazione almeno annuale degli ambiti di trattamento. Nomina anche per classi omogenee di incaricati. (Reg. 27)
- I documenti contenenti dati sensibili o giudiziari sono controllati e custoditi dagli incaricati per tutta la durata di svolgimento delle operazioni e sono restituiti al termine delle operazioni effettuate. (Reg. 28)
- L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Dopo l'orario di chiusura, registrazione delle persone ammesse, a vario titolo ad accedervi. Nel caso di esistenza di un sistema elettronico per il controllo degli accessi, le persone devono essere preventivamente autorizzate. (Reg. 29)

Tabella di comparazione (1/2)

Art. 34 – comma 1	All.B	
	P	S
a) autenticazione informatica	1 → 3	
b) procedure di gestione delle credenziali di autenticazione	4 → 11	
c) sistema di autorizzazione	12 → 14	
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento	15	
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici	16 → 17	20 →22
f) procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi	18	23
g) tenuta di un aggiornato documento programmatico sulla sicurezza		19, 26
h) tecniche di cifratura o di codici identificativi per trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale (org. sanitari)		24

Tabella di comparazione (2/2)

Art. 35 – comma 1	All.B	
	P	S
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative	27	
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;		28
c) previsione di procedure per la conservazione di determinati atti in archivi di accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati	27	29

Gli Amministratori di Sistema (1/2)

- Il Provvedimento a carattere generale del Garante per la Protezione dei Dati Personali del 27.11.2008 titolato ”Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore” introduce l’obbligo di individuare e nominare (per iscritto) i c.d. “**Amministratori di Sistema**”;
- L’ Amministratore di Sistema (AdS) è la figura professionale a cui è conferito, in ambito informatico, il compito di sovrintendere alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti, nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli Amministratori di Sistema (2/2)

- Gli AdS sono individuati, eventualmente anche tra soggetti esterni, in base all'esperienza, alle capacità ed l'affidabilità, nonchè tenendo conto dei relativi profili professionali e delle funzioni concretamente svolte.
- L'elenco degli AdS va mantenuto aggiornato e disponibile in caso di accertamenti da parte del Garante.
- Per ciascun soggetto designato quale AdS dovranno essere specificati analiticamente gli ambiti di operatività, in base allo specifico profilo di autorizzazione assegnato.
- Le funzioni di AdS sono attribuite solo nel quadro di una designazione quale incaricato o responsabile del trattamento.
- Conservazione dei log degli accessi degli AdS ai sistemi gestiti per almeno 6 mesi, in forma completa ed inalterabile e con verifica di integrità.
- Il log deve contenere riferimento temporale e descrizione dell'evento che ha generato la registrazione.

Sistema delle sanzioni

- **Il Codice ha inasprito le sanzioni da applicare in caso di inadempienza del titolare del trattamento.**

- La violazione delle norme sul trattamento dei dati personali comporta può generare:
  1. Responsabilità civile;
  2. Responsabilità amministrativa;
  3. Responsabilità penale.

Responsabilità civile (1/2)

Art. 15: "*chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*".

(**Rinvio all'art. 2050:***"chiunque cagiona ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno".* **Inquadramento dell'attività di trattamento dati personali nell'ambito delle "attività pericolose".**

Conseguenza: applicazione del principio di responsabilità oggettiva e dell'inversione dell'onere della prova:
il danneggiato avrà diritto al risarcimento del danno per il solo fatto di avere subito un pregiudizio derivante dallo svolgimento di attività di trattamento dati personali e non dovrà dimostrare che il danno è stato causato da una condotta negligente del danneggiante; spetta al danneggiante, invece, dimostrare di avere adottato tutte le misure idonee a evitare il danno.

Responsabilità civile (2/2)

- Essenziale, ai fini dell'esclusione della responsabilità, **che i responsabili e per gli incaricati del trattamento osservino scrupolosamente le istruzioni individuate dall'Amministrazione in attuazione della normativa in materia di privacy (oltre a quelle contenute direttamente nel Codice Privacy).**

- Chi può essere responsabile civilmente? "chiunque": titolare, responsabile ed incaricato (anche in solido) in relazione ai rispettivi ambiti di competenza.

Responsabilità amministrativa

La violazione delle disposizioni sul trattamento dei dati personali può dare luogo a responsabilità amministrativa, con applicazione delle relative sanzioni pecuniarie.

Organo competente ad accertare e irrogare la sanzione amministrativa è il **Garante** che emette **ordinanza – ingiunzione motivata di pagamento**, che costituisce titolo esecutivo.

Soggetti responsabili: titolare, responsabili e incaricati, in relazione alle specifiche competenze

Violazioni amministrative e relative sanzioni (1/2)

Art. 161:

- Violazione: **omessa o inidonea informativa all'interessato,**
- Sanzione: **pagamento di una somma da seimila a trentaseimila euro ed eventuale pubblicazione della ordinanza**

Art. 162, rubricato "*Altre fattispecie*"

- Violazioni: **cessione di dati in violazione dell'art. 16 comma 1 lett. B**) ["*i dati sono ceduti ad altro titolare, purchè destinati a un trattamenti in termini compatibili agli scopi per i quali i dati sono raccolti*"] **o in violazione di altre disposizioni in materia di disciplina del trattamento di dati personali**
- Sanzione: **pagamento di una somma da diecimila a sessantamila euro ed eventuale pubblicazione della ordinanza**

Violazioni amministrative e relative sanzioni (2/2)

Art. 163:

- Violazione: **omessa o incompleta notificazione al Garante**
- Sanzione: **pagamento di una somma da ventimila a centomila euro**

Art. 164:

- Violazione: **omessa informazione o esibizione al Garante**
  Sanzione: **pagamento di una somma da diecimila a sessantamila euro ed eventuale pubblicazione della ordinanza**

Art. 164-bis:

- **Sono previsti casi di minore gravità ed ipotesi aggravate**

Art. 165:

- **Può essere applicata la sanzione amministrativa aggiuntiva di pubblicazione dell'ordinanza-ingiunzione su uno o più giornali**

Responsabilità penale

- La violazione delle disposizioni sul trattamento dei dati personali può dare luogo a responsabilità penale, con applicazione delle relative sanzioni.
- **La responsabilità penale è personale. In virtù di questo principio potranno essere penalmente responsabili solo le singole persone fisiche che hanno violato le disposizioni sul trattamento dei dati personali (Rettore, Direttore Amministrativo, Responsabili di Uffici e Strutture e Incaricati)**

Violazioni penali e relative sanzioni (1/3)

Art. 167

- Violazione: **Trattamento illecito di dati**
- Sanzioni differenziate in relazione alle diverse norme violate:
  - **reclusione da sei a diciotto mesi** (**e pubblicazione della sentenza**) se il trattamento avviene, al fine di trarre profitto per sé o per altri, o di recare ad altri un danno, in violazione degli artt. 18, 19, 23, 123, 126, 130 o in applicazione di quanto disposto dall'art. 129, se dal fatto deriva nocumento;
  - **reclusione da sei a ventiquattro mesi** (**e pubblicazione della sentenza**) se il fatto consiste nella comunicazione o diffusione;
  - **Reclusione da uno a tre anni** (**e pubblicazione della sentenza**) se il trattamento avviene in violazione degli artt. 17, 20, 21, 22 commi 8 e 11, 26, 27 e 45, se dal fatto deriva nocumento e se sussiste il fine di trarre vantaggio per sé o per altri o di recare ad altri un danno.

N.B.: la mera violazione delle norme del codice indicate nell'art. 167 comporta la sanzione amministrativa del pagamento di una somma da euro 10.000 a 120.000

Violazioni penali e relative sanzioni (2/3)

Art. 168:

- Violazione: **falsità nelle dichiarazioni o notificazioni al Garante**
- Sanzione: **reclusione da sei mesi a tre anni e pubblicazione della sentenza**

Art. 169:

- Violazione: **omissione nell'adozione delle misure minime di sicurezza**
- Sanzione: **arresto fino a due anni e pubblicazione della sentenza. Viene in ogni caso applicata anche la sanzione amministrativa del pagamento di una somma da diecimila euro a centoventimila euro.** (art. 162 comma 2 bis)

Violazioni penali e relative sanzioni (3/3)

Art. 170:

- Violazione: **Inosservanza dei provvedimenti del Garante**
- Sanzione: **reclusione da tre mesi a due anni e pubblicazione della sentenza**

Art. 171

- Violazione: **inosservanza delle disposizioni di cui all'articolo 113 comma 1 e 114**
- Sanzione: art. 38 legge 300/70 e **pubblicazione della sentenza**