La tutela della privacy e le misure di sicurezza

Ravenna, Facoltà di Giurisprudenza, 4 maggio 2012

Avv. Ph.D. Michele Martoni

Fonti normative e provvedimenti

- Decreto Legislativo 30 giugno 2003, n. 196 (*c.d. Codice Privacy*)
- Direttiva 95/46/CE

- Provvedimenti in www.garanteprivacy.it

Art. 1
Diritto alla protezione

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

Riservatezza e Privacy

Diritto alla riservatezza

diritto di ciascuno «*alla tutela di quelle situazioni personali o familiari svoltesi anche al di fuori del domicilio domestico che non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze non giustificate da interessi pubblici prevalenti, anche se lecite e tali da non offendere l'onore e il decoro. Questo diritto non può essere negato ad alcuna categoria di persone, solo in considerazione della loro notorietà, salvo che un reale interesse sociale all'informazione o altre esigenze pubbliche lo esigano*»

Cass. Civ. n. 2129, 27 maggio 1975, in Foro italiano, 1976, I, 2895

Diritto alla privacy

Il diritto alla privacy, invece, consiste nel diritto di ciascuno di controllare la circolazione delle informazioni riguardanti la propria persona

Rodotà, in Privacy e costruzione della sfera privata. Ipotesi e prospettive, in Politica del diritto, dicembre, 1991

Quali dati ci riguardano ?

- Informazioni personali
  - Dati propri
  - Dati dei propri familiari
  - Dati di terzi
- Informazioni in contesto lavorativo
  - Dati del professionista
  - Dati dell'impresa
  - Dati dei clienti
  - Dati dei cittadini nel caso di pubblica amministrazione

Come condivido i miei dati ?

- Comunicazione diretta
- Comunicazione a molti
  - Gruppi chiusi
  - Aree riservate
  - Amici di amici
  - Cerchie
- Diffusione
- Abbandono

“perdo” di vista i miei dati ?

- Li abbandono ?
- Li cedo senza rendermene conto ?
- Li cedo consapevolmente ma senza attenzione ?
- Li diffondo senza attenzione ?
- Li passo ad amici che poi li diffondono ?
- Li passo ad amici … ad amici di amici … ad amici di amici di amici … ?
- Li gestisco in maniera errata (user id, pw, impostazioni del browser, etc.) ?

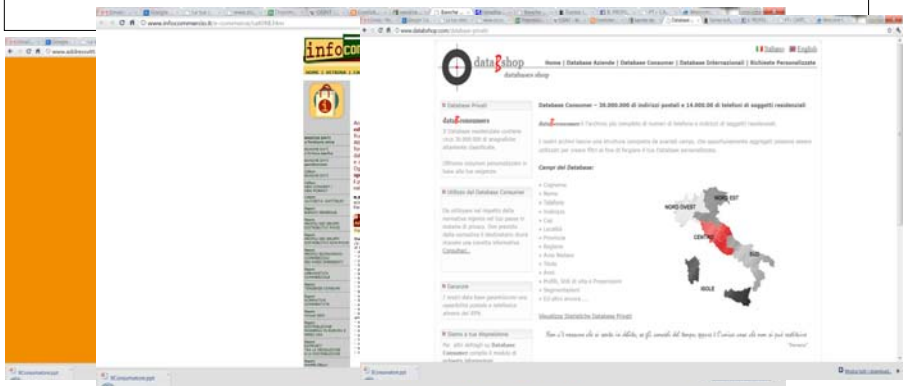
Ingegneria sociale

- Kevin Mitnick “L’arte dell’inganno”
- Jeffery Deaver “La finestra rotta”
- OSINT
  - OSINT, abbreviazione delle parole inglesi **Open Source INTelligence**, è l'attività di raccolta di informazioni mediante ***la consultazione di fonti di pubblico accesso***. Nell'ambito di operazioni di intelligence il termine "Open Source" si riferisce a fonti pubbliche, liberamente accessibili, in contrapposizione a fonti segrete o coperte.

Phishing

[segue]

- Banche dati come forma di business

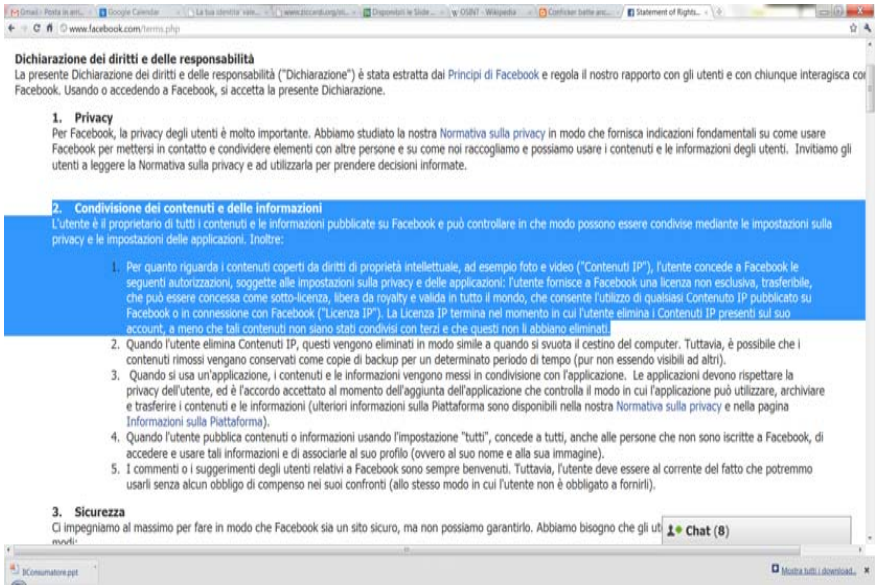


Se non li cedo “consapevolmente”
da dove se ne escono !!!

- **Clausola contrattuale** … che prevede l’impiego per diverse finalità e la comunicazione dei dati (anche) a soggetti terzi

- **Licenza sui contenuti** … video … foto … commenti … etc…

- **Consenso** espresso al trattamento (informativa per il trattamento dei dati personali)



Dichiarazione dei diritti e delle responsabilità

La presente Dichiarazione dei diritti e delle responsabilità ("Dichiarazione") è stata estratta dai Principi di Facebook e regola il nostro rapporto con gli utenti e con chiunque interagisca co Facebook. Usando o accedendo a Facebook, si accetta la presente Dichiarazione.

1. Privacy

Per Facebook, la privacy degli utenti è molto importante. Abbiamo studiato la nostra Normativa sulla privacy in modo che fornisca indicazioni fondamentali su come usare Facebook per mettersi in contatto e condividere elementi con altre persone e su come noi raccogliamo e possiamo usare i contenuti e le informazioni degli utenti. Invitiamo gli utenti a leggere la Normativa sulla privacy e ad utilizzarla per prendere decisioni informate.

2. Condivisione dei contenuti e delle informazioni

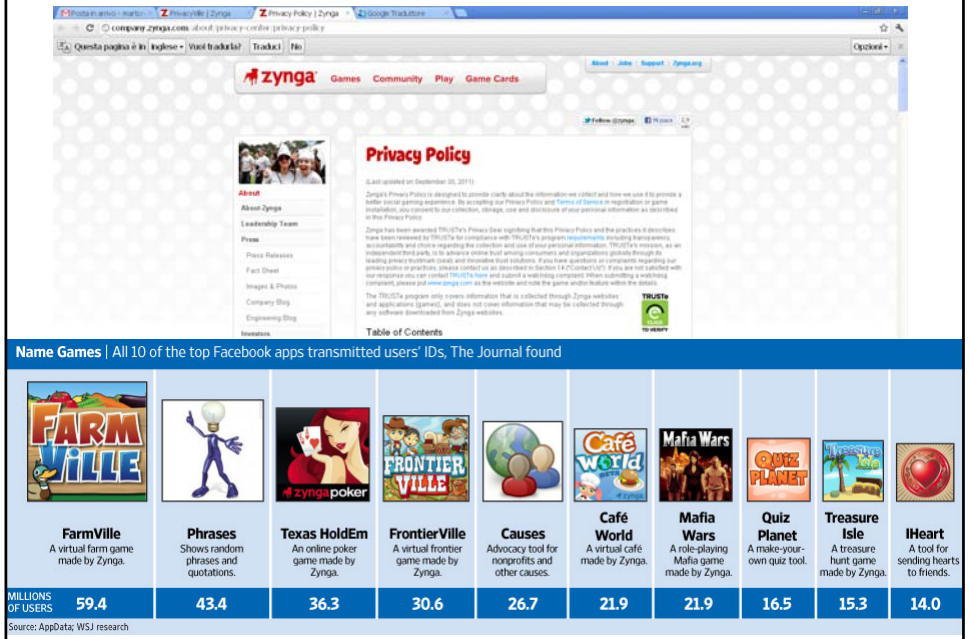
L'utente è il proprietario di tutti i contenuti e le informazioni pubblicate su Facebook e può controllare in che modo possono essere condivise mediante le impostazioni sulla privacy e le impostazioni delle applicazioni. Inoltre:

1. Per quanto riguarda i contenuti coperti da diritti di proprietà intellettuale, ad esempio foto e video ("Contenuti IP"), l'utente concede a Facebook le seguenti autorizzazioni, soggette alle impostazioni sulla privacy e delle applicazioni: l'utente fornisce a Facebook una licenza non esclusiva, trasferibile, che può essere concessa come sotto-licenza, libera da royalty e valida in tutto il mondo, che consente l'utilizzo di qualsiasi Contenuto IP pubblicato su Facebook o in connessione con Facebook ("Licenza IP"). La Licenza IP termina nel momento in cui l'utente elimina i Contenuti IP presenti sul suo account, a meno che tali contenuti non siano stati condivisi con terzi e che questi non li abbiano eliminati.
2. Quando l'utente elimina Contenuti IP, questi vengono eliminati in modo simile a quando si svuota il cestino del computer. Tuttavia, è possibile che i contenuti rimossi vengano conservati come copie di backup per un determinato periodo di tempo (pur non essendo visibili ad altri).
3. Quando si usa un'applicazione, i contenuti e le informazioni vengono messi in condivisione con l'applicazione. Le applicazioni devono rispettare la privacy dell'utente, ed è l'accordo accettato al momento dell'aggiunta dell'applicazione che controlla il modo in cui l'applicazione può utilizzare, archiviare e trasferire i contenuti e le informazioni (ulteriori informazioni sulla Piattaforma sono disponibili nella nostra Normativa sulla privacy e nella pagina Informazioni sulla Piattaforma).
4. Quando l'utente pubblica contenuti o informazioni usando l'impostazione "tutti", concede a tutti, anche alle persone che non sono iscritte a Facebook, di accedere e usare tali informazioni e di associarle al suo profilo (ovvero al suo nome e alla sua immagine).
5. I commenti o i suggerimenti degli utenti relativi a Facebook sono sempre benvenuti. Tuttavia, l'utente deve essere al corrente del fatto che potremmo usarli senza alcun obbligo di compenso nei suoi confronti (allo stesso modo in cui l'utente non è obbligato a fornirli).

3. Sicurezza

Ci impegniamo al massimo per fare in modo che Facebook sia un sito sicuro, ma non possiamo garantirlo. Abbiamo bisogno che gli ut

Chat (8)



http://company.zynga.com/about/privacy-center/privacy-policy

Norme sulla Privacy Google (2012)

- https://www.google.it/intl/it/policies/

Annunci sul web
Google

consapevolezza

... leges sine moribus vanae ...

(Pennsylvania University)

disvalore

- Se non comprendo il **valore tutelato** (ad esempio la riservatezza del dato piuttosto che la certezza della identità di una persona) sarò portato a **non applicare** e quindi a non rispettare la disciplina in materia
- Sarò portato a vivere come un **inutile appesantimento** tutto ciò che viene sancito e regolamentato
- **Giustificherò-Legalizzerò** la **illegalità**

cosa intendo dire:

consapevole di cosa?

1) del valore del dato

- **<u>per l'interessato</u>**
- **<u>per altri soggetti</u> (valore oggettivo)**

Quello che vale viene rubato dunque Quello che viene rubato vale

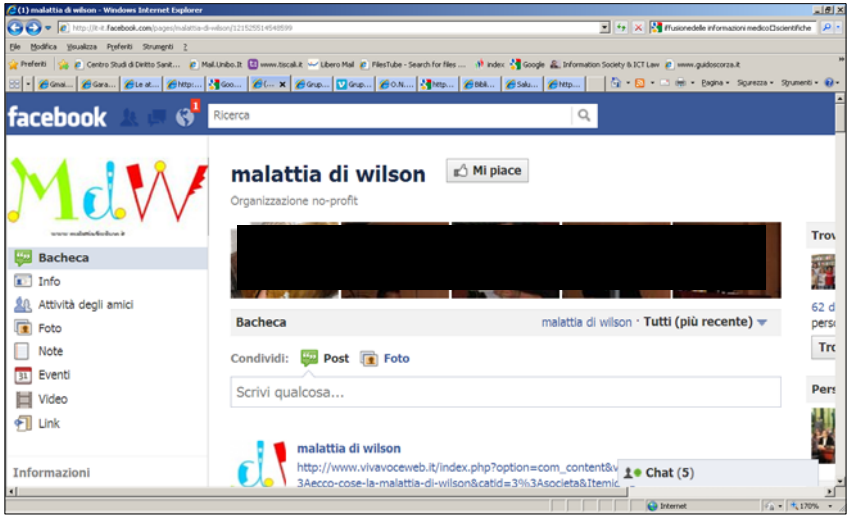
1. Geisinger Health System (Danville, Pa.)
2. Dean and St. Mary's Hospital (Madison, Wis.)
3. Mountain Vista Medical Center (Mesa, Ariz.)
4. University of Tennessee Medical Center (Knoxville, Tenn.)
5. Kern Medical Center (Bakersfield, Calif.)
6. New York-Presbyterian Hospital (New York City)
7. Thomas Jefferson University Hospital (Philadelphia)
8. Griffin Hospital (Derby, Conn.)
9. South Shore Hospital (Weymouth, Mass.)
10. Johns Hopkins Hospital (Baltimore)
11. North Central Bronx Hospital
12. Beebe Medical Center
13. Queen Mary Hospital
14. Calderdale and Huddersfield
15. ecc...ecc...ecc...

consapevole di cosa?

2) degli strumenti impiegati

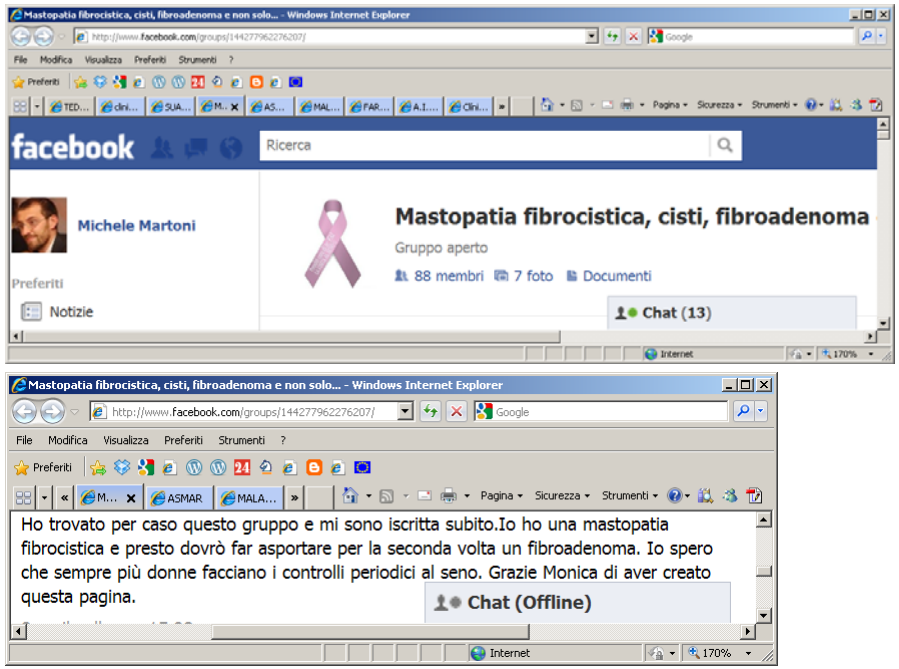
- **delle caratteristiche di funzionamento e delle finalità**
- **delle condizioni d'uso**
- **dei limiti degli strumenti**

cosa intendo dire:




facebook
Ricerca
Incontinenza urinaria (Urinary incontinence)
Mi piace
Malattie · Intendevi Incontinenza urinaria (Italiano)?
Post correlati
Wellness Briefs
You have asked Why the Wellness Brief Adult Diaper? and we have answered:
http://bit.ly/hXwPGr Urinary incontinence
Why Unique Wellness As The Number One Choice for Adult Diapers « Wellness Briefs Official Informati
wellnessbriefs.wordpress.com
Space Age Technology The Unique Wellness® incontinence program is based on the same principles as the Maximum Absorbency Garments (MAGs) developed by NASA. (click here to see how The Unique Wellness program is based on NASA technology)
Info
Attività degli amici
Post correlati
Wikipedia
241
di "Mi piace"
Chat (5)


Ricerca
MALATTIA DI MENIERE ▸ Documenti
Torna alla bacheca
Invalidità
di Maledetta Menière e [redacted]
[redacted]
Salve a tutti. Purtroppo io non potrò esserci a Bologna e vorrei porre dei quesiti circa l'inavalidità, visto che sarà oggetto di discussione. Io per orgoglio o vergogna non ho mai chiesto l'invalidità anche se molti cercano di farmi capire che in fondo è un mio diritto. Io la vedo ancora come una sconfitta. Per me è come se ave...
Ultima modifica circa 2 mesi fa
Chat (8)



basterebbe non rendere pubblica la bacheca !

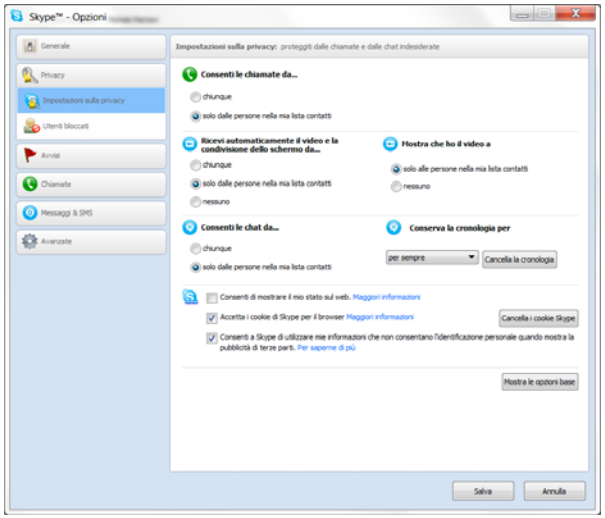
Posta con la Testa

- **Posta con la testa (Insafe)**
- http://www.youtube.com/watch?v=sNEVYUT1Tio
- **What you post can haunt you forever**
- http://www.youtube.com/watch?v=Enph-DJ7wv0&feature=related
- **Once posted you lose it**
- http://www.youtube.com/watch?v=CE2Ru-jqyrY&feature=related

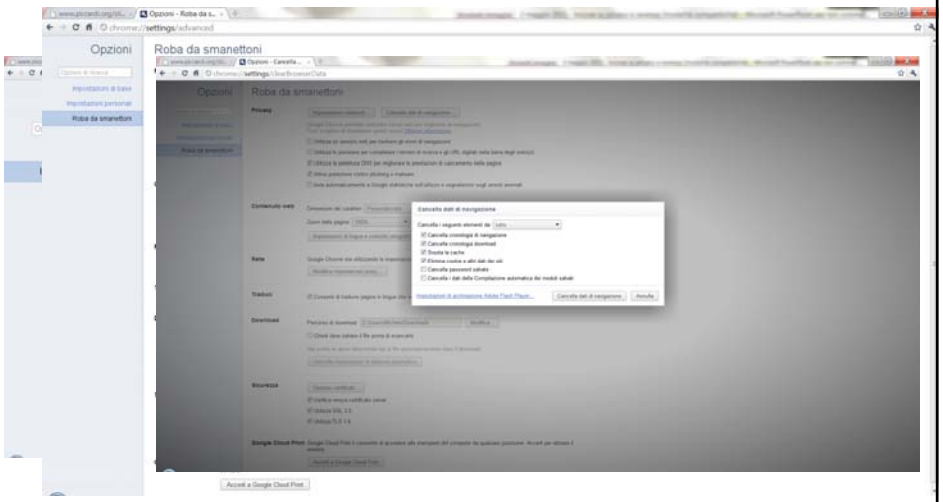
Privacy e applicazioni

- Oggi la maggior parte delle applicazioni o dei servizi hanno una “sezione” che consente delle scelte in tema di privacy.
- Si pensi, ad esempio, alle preferenze dei browser (che vanno ad agire su cronologia, cache, cookies) o ai servizi sul web (quali ad esempio Facebook ma anche Skype, Messenger o simili) che permettono di impostare il servizio più o meno “restrittivo” con riferimento alla privacy del soggetto utilizzatore [G. Ziccardi]

Esempio “Skype”



Esempio “Chrome”



Cosa fare (?)

- Consapevolezza sul valore delle proprie informazioni
- Conoscenza ed impostazione attenta dei propri strumenti : pc, smartphone, etc…
- Uso attento e consapevole dei servizi online … leggere con attenzione “tutto”
- Scegliere con attenzione strumenti e software
- e in ogni caso tenere sempre presente … che i sistemi e le persone … sono vulnerabili

coffee break !

Il quadro normativo

Art. 1
Diritto alla protezione dei dati personali

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

Art. 4 Definizioni *“interessato”*

i) Si intende per *interessato*, la persona fisica, la persona giuridica, l’ente o l’associazione cui si riferiscono i dati personali.

“persone giuridiche”

- Il Decreto Legge 6 dicembre 2011, n. 201 (in G.U. n. 284 del 6 dicembre 2011 - Suppl. Ord. n. 251 - in vigore dal 6 dicembre 2011), recante "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici" (c.d Decreto "salva-Italia"), all'articolo 40 ha introdotto importanti novità in tema di trattamento dei dati personali delle persone giuridiche.

Segnatamente, il comma 2 dispone che:

"2. Per la riduzione degli oneri in materia di privacy, sono apportate le seguenti modifiche al decreto legislativo 30 giugno 2003, n. 196: a) all'articolo 4, comma 1, alla lettera b), le parole "**persona giuridica, ente od associazione**" sono soppresse e le parole "identificati o identificabili" sono sostituite dalle parole "identificata o identificabile". b) All'articolo 4, comma 1, alla lettera i), le parole "la persona giuridica, l'ente o l'associazione" sono soppresse. c) Il comma 3-bis dell'articolo 5 è abrogato. d) Al comma 4, dell'articolo 9, l'ultimo periodo è soppresso. e) La lettera h) del comma i dell'articolo 43 è soppressa.“

Art. 4 Definizioni *"trattamento"*

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

Art. 2
Finalità

1. … il trattamento dei dati personali *si svolge* nel rispetto dei **diritti e delle libertà fondamentali**, nonché della **dignità dell'interessato**, con particolare riferimento alla **riservatezza**, **all'identità personale** e al **diritto di protezione dei dati personali.**

Considerazioni

- Il ***comma 1*** definisce l'orizzonte dei valori e dei beni giuridici entro cui si muove questa normativa

Considerazioni

- Il diritto alla **riservatezza** (ovvero la protezione della vita privata)
- Il diritto alla **identità personale** (ovvero la protezione della individualità di ciascuno, che si attua anche tramite la tutela delle informazioni che precisano i contorni della individualità
- Il diritto alla **protezione dei dati personali**

Considerazioni

- Diritto di ciascuno a che i propri dati personali, ove trattati da un'altra persona, siano protetti con le modalità e secondo gli *standard* definiti dalla legge
- Patrimonio informativo di ciascuno come patrimonio informativo **circolante**, sottoposto ad uso da tanti soggetti per le finalità più varie

Art. 5
Oggetto ed ambito di applicazione

1. … disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in luogo comunque soggetto alla sovranità dello Stato
2. … si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato … salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione …
3. … trattamento di dati personali effettuato da persone fisiche **per fini esclusivamente personali** è soggetto alla applicazione del presente codice **solo se** i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

Considerazioni:
Fini esclusivamente personali

- Si ritiene che diffusione dei dati e fini personali non siano compatibili (esclusa configurabilità di uno scopo personale in caso di diffusione dei dati)
- La deroga vi è nell'area in cui ciascun individuo apprende notizie e informazioni che rimangono utilizzate in una dimensione strettamente privata.

Considerazioni:
Fini esclusivamente personali

- La legge tutela le persone cui si riferiscono i dati ma rispetta anche la sfera personale di chi intenda esercitare la libertà di informarsi e di essere informato per perseguire scopi meramente personali.
- Inapplicabile (tranne artt. 15 e 31) alle agende automatizzate e cartacee, alle rubriche, agli indirizzari, agli appunti e al materiale informativo che chiunque è solito conservare nella propria sfera privata per soddisfare interessi culturali o altre normali esigenze della vita di relazione.

Considerazioni:
Comunicazione sistematica

- Si riferisce alla sola comunicazione, non alla diffusione: o per soddisfare le proprie esigenze personali o se viene effettuata una comunicazione saltuaria ed episodica

- Attenzione: si riferisce solo alla persona fisica: il soggetto che tratta i dati deve essere una persona fisica. Non riguarda le aziende.

Art. 4 Definizioni *"comunicazione"*

l) Si intende per *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.

Art. 4 Definizioni *“diffusione”*

m) Si intende per *diffusione*, il dare conoscenza dei dati personali **a soggetti indeterminati**, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 4 Definizioni *“dato personale”*

b) Si intende per *dato personale*, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Art. 4 Definizioni *“dati identificativi”*

c) Si intende per *dati identificativi*, i dati personali che permettono l’identificazione **diretta** dell’interessato.

Art. 4 Definizioni *“dati sensibili”*

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

Art. 4 Definizioni *“dati giudiziari”*

e) Si intende per *dati giudiziari*, i dati personali idonei a rivelare provvedimenti di cui all’articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Art. 4 Definizioni *“titolare”*

f) Si intende per *titolare*, la persona fisica, la persona giuridica, la pubblica amministrazione e qualunque altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza.

Art. 28
Titolare del trattamento

1. Quando il trattamento è effettuato da una persona giuridica, da una **pubblica amministrazione** o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo di sicurezza.

Art. 4 Definizioni *"responsabile"*

g) Si intende per *responsabile*, la persona fisica, la persona giuridica, la pubblica amministrazione e qualunque altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.

Art. 29
Responsabile del trattamento

1. Il responsabile è designato dal titolare **facoltativamente**.
2. Se designato, il responsabile 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.
3. Ove necessario per esigenze organizzative, possono essere designati responsabili **più soggetti**, anche mediante suddivisione dei compiti.
4. I compiti affidati al responsabile sono analiticamente specificati **per iscritto** dal titolare.
5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, …, **vigila** sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Considerazioni
Responsabile del trattamento

- Rispecchia l'art. 1, lett. *e*, L. 675/1996
- Nomenclatura comunitaria
- Profilo soggettivo ampio
- Soggetto facoltativo (interno o esterno)
- Soggetto con specifiche capacità
- Delega di funzioni e responsabilità
- Nomina di più soggetti
- Formalità per la nomina

Art. 4 Definizioni *“incaricati”*

h) Si intendono per *incaricati*, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Art. 30
Incaricati del trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano **sotto la *diretta* autorità** del titolare o del responsabile, attenendosi alle istruzioni impartite.
2. La designazione è effettuata **per iscritto** e individua puntualmente l’ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, **per iscritto**, l’ambito del trattamento consentito agli addetti all’unità medesima.

Considerazioni
Incaricati del trattamento

- Modifiche rispetto alla L. 675/1996
- Autorizzazione al trattamento
- Nomina da parte del Titolare o del Responsabile
- Istruzioni specifiche e controllo
- Forma scritta della nomina
- Soggetto interno o esterno alla struttura
- Responsabilità

Art. 3
Principio di necessità

1. 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 od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 11
Modalità del trattamento e requisiti

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) 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.

Art. 37
Notificazione

- https://web.garanteprivacy.it/rgt/NotificaEsplora.php
- a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.
- Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta Ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.
- Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

Art. 13
Informativa

1. 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;

Art. 13
Informativa

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.

Art. 13
Informativa

2. L’informativa di cui al comma 1 contiene anche gli elementi previsti da **specifiche disposizioni** del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l’espletamento, da parte di un soggetto pubblico, di **funzioni ispettive o di controllo** svolte per finalità di difesa o di sicurezza dello Stato oppure di **prevenzione**, **accertamento o repressione di reati**.

Art. 13
Informativa

3. Il Garante può individuare con proprio provvedimento **modalità semplificate** per l’informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.
4. Se i dati personali **non sono raccolti presso l’interessato**, l’informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all’atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

Art. 13
Informativa

5. La disposizione di cui al comma 4 non si applica quando:
   a) i dati sono trattati in base ad **un obbligo previsto dalla legge**, da un regolamento o dalla normativa comunitaria;
   b) i dati sono trattati ai fini dello svolgimento delle **investigazioni difensive** di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
   c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

Art. 23
Consenso

1. Il trattamento di dati personali da parte di **privati o di enti pubblici** economici è ammesso solo con il consenso **espresso** dell'interessato.
2. Il consenso può riguardare **l'intero trattamento** ovvero **una o più operazioni** dello stesso.
3. Il consenso è validamente prestato solo se è **espresso liberamente e specificamente** in riferimento ad un **trattamento chiaramente individuato**, se è **documentato per iscritto**, e se sono state rese all'interessato le **informazioni di cui all'articolo 13**.
4. Il consenso è manifestato in **forma scritta** quando il trattamento riguarda **dati sensibili**.

Art. 24
Casi in cui non occorre il consenso

1. Il consenso **non è richiesto**, oltre che nei casi previsti nella Parte II, quando il trattamento:

   - è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
   - è necessario per eseguire obblighi derivanti da un contratto …;

…

- riguarda dati provenienti da **pubblici registri**, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

...

- è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

...

- **con esclusione della diffusione**, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

...

- **con esclusione della diffusione**, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

...

- **con esclusione della comunicazione all'esterno e della diffusione**, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

…

- è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

Art. 26
Garanzie per i dati sensibili

1. I dati sensibili possono essere oggetto di trattamento solo con il **consenso scritto** dell'interessato **e** previa **autorizzazione** del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.
2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

Art. 26
Garanzie per i dati sensibili

3. Il **comma 1 non si applica** al trattamento:

a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

Art. 26
Garanzie per i dati sensibili

4. I dati sensibili possono essere oggetto di trattamento **anche senza consenso**, **previa autorizzazione** del Garante:

a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

Art. 26
Garanzie per i dati sensibili

b) **quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo**. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

Art. 26
Garanzie per i dati sensibili

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

Art. 26
Garanzie per i dati sensibili

d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

5. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

Art. 27
Garanzie per i dati giudiziari

1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

Art. 7
Diritto di accesso ai dati 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.

Art. 7
Diritto di accesso ai dati ed altri diritti

2. L'interessato ha diritto di ottenere l'indicazione:
   - dell'**origine** dei dati personali;
   - delle **finalità** e **modalità** del trattamento;
   - della **logica** applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   - degli **estremi identificativi del titolare**, dei responsabili e del rappresentante designato sul territorio …;
   - 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.

Art. 7
Diritto di accesso ai dati ed altri diritti

3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, *eccettuato* il caso in cui tale adempimento si riveli impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

Art. 7
Diritto di accesso ai dati ed altri diritti

4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per **motivi legittimi** al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di **materiale pubblicitario** o di **vendita diretta** o per il compimento di **ricerche di mercato** o di **comunicazione commerciale**.

Considerazioni

- Riprende vecchio art. 13 L. 675/1996 con sola novità comma 1 lettera *e*) (che aggiunge fra le attribuzioni dell'interessato il diritto di conoscere i soggetti ai quali i dati possono essere comunicati o che ne possono comunque venire a conoscenza.
- La tutela dei diritti dell'interessato è il primo di tre requisiti di effettività della normativa, insieme ai controlli del Garante ed alla tutela amministrativa e giurisdizionale

Considerazioni

- Due contrappesi: dovere del Titolare di FAR SAPERE (informativa) e diritto dell'interessato di SAPERE.
- L'interessato ha anche però diritto di conoscere l'origine dei dati personali e la logica applicata al trattamento automatizzato, cui la disciplina dell'informativa non fa riferimento.

Considerazioni

- Collaborazione dell'interessato: ha la responsabilità di fare quanto possibile per facilitare la ricerca, principio di correttezza e buona fede che deve conformare tutte le parti in causa (specificazione di elementi che agevolino la ricerca, periodo di riferimento etc etc)

Considerazioni:
I diritti di conoscenza

- Accesso dell'interessato per sapere se una organizzazione trattiene dati personali che lo riguardano
- Diritto di informarsi: posizione attiva dell'interessato
- Due modalità di diritto di accesso: accesso presso il registro Pubblico, consultabile su base territoriale diffusa, gratuitamente e senza l'onere di particolari formalità e accesso presso il titolare o il Responsabile del Trattamento.

Considerazioni
Le richieste

- Se esistono o meno dati che lo riguardano (si può esercitare anche nei confronti di chi potrebbe non essere Titolare di alcun trattamento dei nostri dati)
- Permettono di identificare violazioni alla trasparenza (non era stata data informativa) e di venire a conoscenza di terzi che trattano i nostri dati e che noi ignoravamo (titolare che acquisisce dati da terze parti e magari è esonerato dall'obbligo di legge di informativa - cfr. art. 13.5)

Considerazioni
"anche" *dati non registrati*

- Per evitare scuse da parte del titolare che i dati non sono ancora registrati al fine di eludere la normativa

Considerazioni
La fonte dei dati

- Non si capisce se ci si riferisce al soggetto specifico che ha fornito i dati o alla categoria di soggetti
- A volte può essere molto impegnativo tenere sempre a mente la fonte individuale dei dati: l'articolo dice che il Titolare può anche indicare "le categorie di soggetti"
- L'interessato ricostruisce il flusso informativo del dato

Considerazioni
La logica del trattamento

- Insieme dei principi delle tabelle che definiscono funzioni logiche di una applicazione e dei collegamenti logici utilizzati per eseguire una computazione mediante un sistema di elaborazione automatica di dati.
- E' il criterio informatico di elaborazione dei dati

Art. 8
Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con **richiesta** rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito **idoneo** riscontro **senza ritardo**.
2. I diritti di cui all'articolo 7 **non** possono essere esercitati … se i trattamenti sono effettuati *nelle specifiche ipotesi di cui al comma 2, articolo 8* (vdns.) (es. da commissioni parlamentari di inchiesta, in materia di sostegno alle vittime di richieste estorsive, in materia di riciclaggio, ecc…).

Art. 9
Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante **lettera raccomandata**, **telefax** o **posta elettronica**. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche.

   Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche **oralmente** e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, **delega o procura** a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

Art. 9
Modalità di esercizio

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti **persone decedute** possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. 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.

Art. 9
Modalità di esercizio

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere **rinnovata**, salva l'esistenza di giustificati motivi, con intervallo non minore di **novanta giorni**.

Art. 10
Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare **idonee misure** volte, in particolare:

   a) ad **agevolare l'accesso** ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi *programmi per elaboratore* finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;

   b) a **semplificare** le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

Art. 10
Riscontro all'interessato

2. I dati sono **estratti** a cura del *responsabile* o degli *incaricati* e possono essere comunicati al richiedente anche *oralmente*, ovvero *offerti in visione* mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. **Se vi è richiesta**, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

Art. 10
Riscontro all’interessato

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una **professione sanitaria** o ad **un organismo sanitario** si osserva la disposizione di cui all'articolo 84, comma 1.
4. Quando **l'estrazione** dei dati *risulta particolarmente difficoltosa* il riscontro alla richiesta dell'interessato può avvenire anche attraverso **l'esibizione** o la consegna in copia ~~di atti e documenti contenenti i dati personali richiesti~~.

Art. 10
Riscontro all’interessato

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a **terzi**, *salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.*
6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di **codici o sigle** sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

Art. 10
Riscontro all'interessato

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) **non risulta confermata l'esistenza di dati** che riguardano l'interessato, può essere chiesto un **contributo spese** non eccedente i *costi effettivamente sopportati* per la ricerca effettuata nel caso specifico.

Art. 10
Riscontro all'interessato

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il ***medesimo provvedimento il Garante*** può prevedere che il contributo possa essere chiesto quando i dati personali figurano **su uno speciale supporto** del quale è richiesta specificamente la **riproduzione**, *oppure* quando, presso uno o più titolari, si determina un **notevole impiego di mezzi** in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

Art. 10
Riscontro all’interessato

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque **non oltre quindici giorni** da tale riscontro.

Art. 16
Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:
   a) distrutti;
   b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
   d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.
2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

Art. 14
Definizione di profili e della personalità

1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.
2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17.

Art. 15
Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Capo I - Misure di sicurezza
Art. 31 Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, **in modo da ridurre al minimo**, mediante **l'adozione di idonee e preventive misure** di sicurezza, i rischi di **distruzione o perdita**, anche *accidentale*, dei dati stessi, di **accesso non autorizzato** o di **trattamento non consentito** o **non conforme** alle finalità della raccolta.

Capo II - Misure minime di sicurezza
Art. 33 Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento **sono comunque tenuti** ad adottare le *misure minime* individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34
Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

   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;

Art. 34
Trattamenti con 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.

Art. 35
Trattamenti senza strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

   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 ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36
Adeguamento

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Allegato B.
Disciplinare tecnico (con strumenti elettronici)

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

- *Sistema di autenticazione informatica*
- *Sistema di autorizzazione*
- *Altre misure di sicurezza*
- *Documento programmatico sulla sicurezza*
- *Ulteriori misure in caso di trattamento di dati sensibili o giudiziari*
- *Misure di tutela e garanzia*

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di **credenziali di autenticazione** che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un **codice per l'identificazione dell'incaricato associato a una parola chiave riservata** conosciuta solamente dal medesimo oppure in un **dispositivo** di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le **istruzioni** impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Sistema di autenticazione informatica

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno **otto caratteri** oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Sistema di autenticazione informatica

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive **disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato** che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione **non si applicano ai trattamenti dei dati personali destinati alla diffusione**.

Sistema di autorizzazione

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

Altre misure di sicurezza

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

Documento programmatico sulla sicurezza

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

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

Documento programmatico sulla sicurezza

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di **soggetti esterni** alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella **relazione accompagnatoria** del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Allegato B.
(Trattamenti senza strumenti elettronici)

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

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

Il Garante

domande ?

michele[dot]**martoni**[at]**unibo**[dot]**it**