

Sassari - 27 maggio 2015

La privacy e il Professionista

Avv. Francesco Paolo Micozzi



Menu

- ✱ *I soggetti*
- ✱ *L'informativa Cookies*
- ✱ *Il consenso*
- ✱ *Misure minime di sicurezza*
- ✱ *L'amministratore di sistema*

Quali soggetti?

Necessari

L'interessato

Il titolare

Eventuali

Il responsabile

L'incaricato

I terzi



Interessato

i) "interessato", la persona fisica cui si riferiscono i dati personali

L'interessato è la persona fisica i cui dati personali siano trattati nell'ambito dei limiti stabiliti dall'art. 5.

In quest'ottica sono dati personali quelli riconducibili ad un soggetto o ad una sua qualità

I diritti dell'Interessato (artt. 7-10)

*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.*

I diritti dell'Interessato (7)

*L'interessato ha diritto di **ottenere l'indicazione:***

- a) dell'origine dei dati personali;*
- b) delle finalità e modalità del trattamento;*
- c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;*
- d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;*
- e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.*

I diritti dell'Interessato (7)

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 rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.*

I diritti dell'Interessato (7)

*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.*

Esercizio dei diritti (8)

I diritti precedentemente esposti sono esercitati dall'interessato senza bisogno di alcuna formalità, essendo sufficiente la richiesta al titolare o al responsabile del trattamento.

Esistono, tuttavia, alcuni limiti all'esercizio dei diritti di cui all'art. 7. Questi limiti, generalmente, sono dovuti a ragioni di ordine pubblico, di politica monetaria e valutaria, giudiziarie... In questi casi occorre rivolgersi al Garante – il quale procederà agli accertamenti del caso – e non al titolare o al responsabile del trattamento.

Esercizio dei diritti

La richiesta rivolta al titolare può esser fatta anche con raccomandata, telefax o posta elettronica. Altri strumenti idonei potranno essere, in futuro, individuati dal Garante.

L'esercizio dei diritti di cui all'art. 7 può esser delegato dall'interessato ad altra persona fisica, ente, associazione o organismo.

Per essere identificati, basta allegare copia del documento d'identità (o della delega)

Riscontro all'interessato

Il titolare del trattamento deve fare in modo di:

- agevolare l'accesso ai dati personali da parte dell'interessato
- semplificare modalità e ridurre i tempi d'accesso



**La comunicazione
deve avvenire
in forma intellegibile**

Il Titolare del Trattamento

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

Il Titolare del Trattamento

Art. 28. Quando il trattamento è effettuato da una persona giuridica, da una PA o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità o organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Funzioni del Titolare

Le decisioni strategiche sul trattamento dei dati personali spettano al titolare, anche se egli abbia nominato uno o più responsabili.

Gli obblighi o le responsabilità attribuite dalla legge sono imputate al titolare.

Compiti fondamentali (e inderogabili) del titolare sono quelli di organizzare e vigilare sul processo di trattamento dei dati

Compiti del Titolare

Spetta al titolare:

- ☒ Nominare per iscritto il/i responsabile/i affidandogli in modo analitico e dettagliato i compiti da svolgere nell'ambito del trattamento dei dati
- ☒ Art. 29 comma quarto. Il titolare impartisce per iscritto le istruzioni al responsabile
- ☒ Vigilare sul corretto espletamento dei compiti da parte del/dei responsabile/i
- ☒ Art. 37. Il titolare notifica al Garante il trattamento di dati personali cui intenda procedere qualora riguardino dati indicati dallo stesso articolo.
- ☒ Eseguire le comunicazioni di cui all'art. 39 al Garante.

Delega della Titolarità

La titolarità del trattamento dei dati non è delegabile.



Responsabilità del Titolare

Sul Titolare incombono una serie di responsabilità **amministrative, civili e penali** nelle quali, pur in presenza di responsabili del trattamento, potrebbe incorrere per *culpa in vigilando* o per *culpa in eligendo*.

Il tema delle responsabilità sarà trattato in seguito in maniera più approfondita

Il Responsabile del Trattamento

Il Responsabile è la persona fisica, la persona giuridica, la PA e qualsiasi altro ente, associazione od organizzazione preposti dal titolare al trattamento di dati personali.

La nomina del Responsabile è facoltativa, ma se designato deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano garanzia idonea del pieno rispetto delle disposizioni in materia di trattamento dei dati e sicurezza nel trattamento medesimo.

Il Responsabile

Le esigenze organizzative possono portare alla nomina di più di un responsabile, anche mediante la suddivisione dei compiti

I compiti sono affidati in forma scritta ed indicati analiticamente.

Il titolare vigila sul corretto svolgimento del trattamento dei dati da parte del Responsabile.

“Responsabilità del Responsabile”

Quando il titolare nomina un responsabile,
distribuisce — guardacaso — anche le responsabilità
di natura penale.

Residuano, tuttavia, in capo al titolare le responsabilità
già esposte in precedenza.



Compiti del Responsabile

Procedere al trattamento dei dati secondo quanto impartitogli in forma **scritta** ed **analiticamente** dal Titolare del trattamento

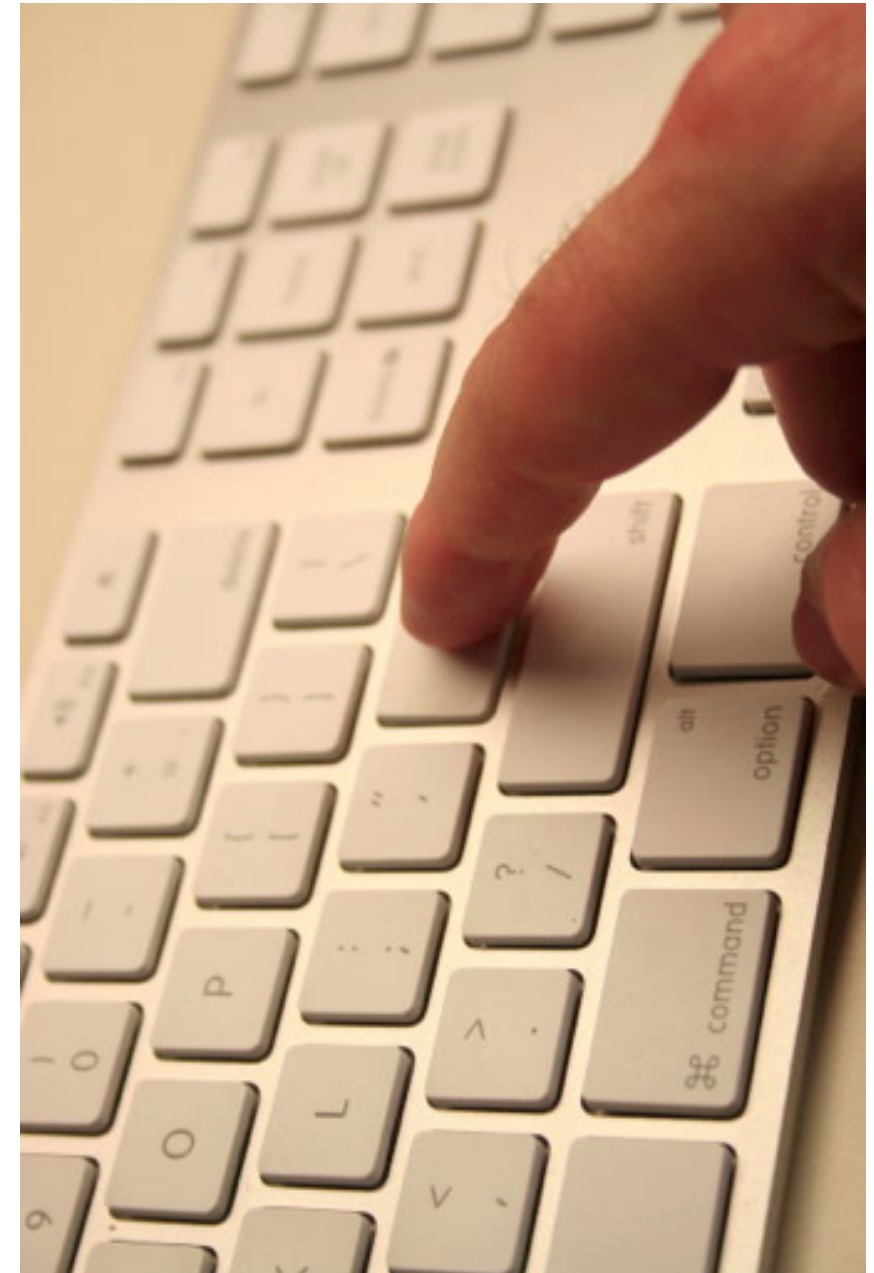
Procedere alle nomine degli incaricati del trattamento

Quest'ultimo compito può essere svolto anche dallo stesso Titolare

Gli Incaricati del Trattamento

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

Incaricati possono essere solamente persone fisiche



Gli Incaricati del Trattamento



Gli incaricati eseguono le operazioni di trattamento attenendosi scrupolosamente a quanto impartito loro dal titolare o dal responsabile

Designazione degli Incaricati

Anche la designazione degli incaricati è fatta per forma scritta ed individua in modo puntuale i compiti loro spettanti.

I compiti possono essere circoscritti anche sulla base delle attività spettanti all'unità organizzativa cui sono preposti

Caratteristiche degli incaricati

Gli incaricati, per loro natura, non hanno alcuna autonomia decisionale, relativamente al trattamento dei dati, rispetto al titolare o al responsabile. Essi non possono prendere sul **perché** e sul **come** utilizzare dei dati.

Possono solo decidere le modalità tecniche per svolgere il servizio loro affidato.

Con l'individuazione degli incaricati si ha un conferimento di compiti specifici sul trattamento dei dati.

I Terzi

Sono i soggetti estranei all'ambito del corretto trattamento dei dati personali

L'informativa

Caratteristiche degli incaricati

Art. 13 del Codice

Cardine della disciplina (e condizione per la prestazione del consenso)

Deve precedere il trattamento

Può essere data sia oralmente che per iscritto

Contenuto dell'informativa

L'informativa deve contenere indicazioni circa:

- le finalità e le modalità del trattamento;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- 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;
- i diritti dell'interessato;
- L'identificazione del titolare e del responsabile

Informativa e CV (art. 13, c. 5-bis)

L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro.

Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f).



Home



Notifiche



Messaggi



Cerca su Twitter



Tweet

Per offrirti Twitter nel modo in cui ti serve, noi e i nostri partner usiamo i cookie sui nostri siti web e su quelli di altri. I cookie consentono di personalizzare i contenuti di Twitter, personalizzare gli Annunci Twitter e misurarne il risultati, nonché offrirti un'esperienza Twitter potenziata, più veloce e più sicura. Usando i nostri servizi, accetti il nostro [Uso dei cookie](#).



Che c'è di nuovo?



Chi seguire · Aggiorna · Visualizza tutto

direttiva 2009/136/CE > d.lgs. 69/2012...

Art. 122. Informazioni raccolte nei riguardi del contraente o dell'utente

1. L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3.

direttiva 2009/136/CE > d.lgs. 69/2012...

Art. 122. Informazioni raccolte nei riguardi del contraente o dell'utente

*1.... Ciò non vieta l'eventuale **archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio.** Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente.*

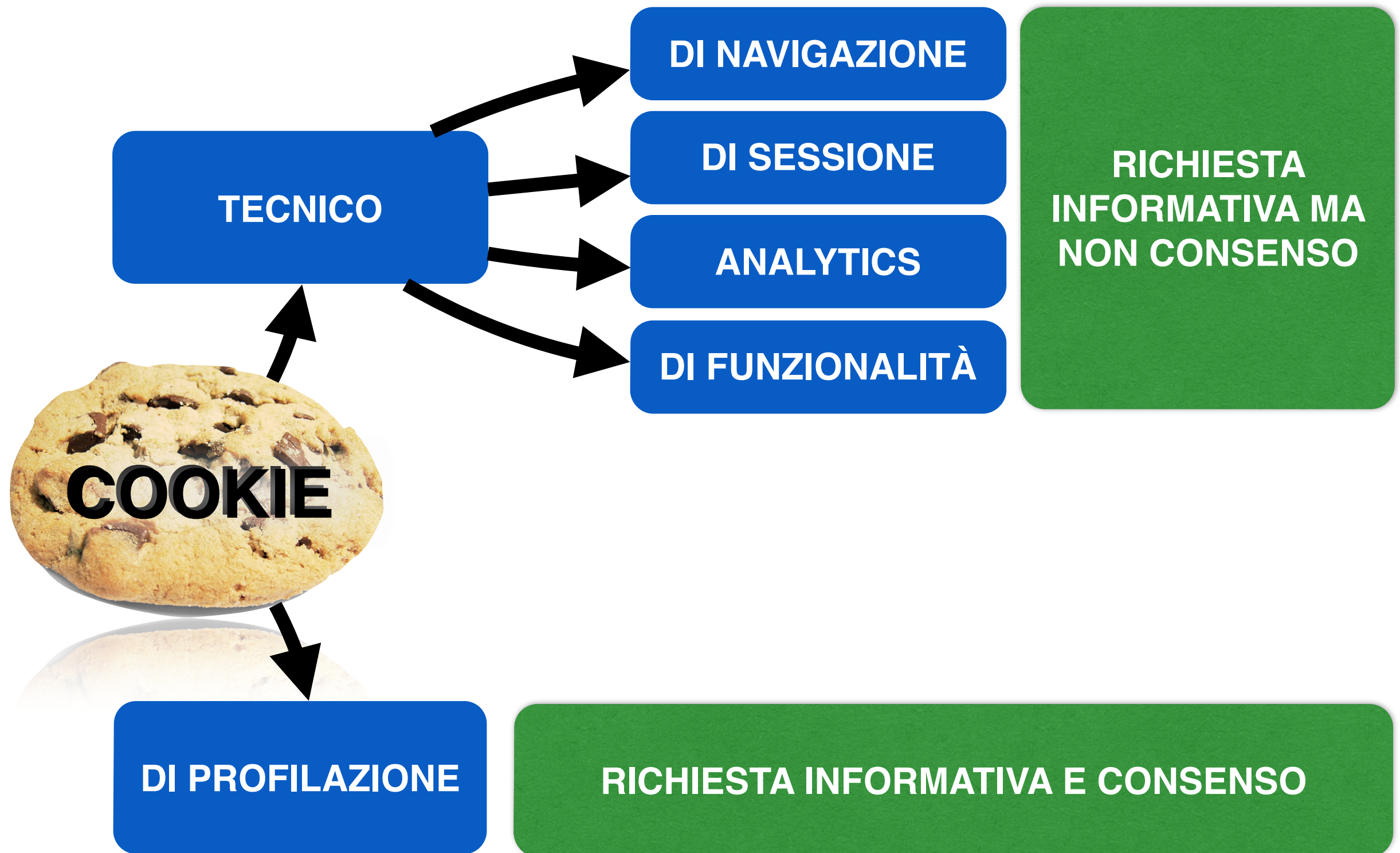
direttiva 2009/136/CE > d.lgs. 69/2012...

Art. 122. Informazioni raccolte nei riguardi del contraente o dell'utente

2. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.

2-bis. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014



Riferimenti - Cookies

- Direttiva europea 2009/136/CE
- D.lgs. 69/2012
- Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014
- Faq in materia di cookie

Il Consenso

Il Consenso (24)

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.



Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

Il Consenso (24)

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.

Il consenso è **manifestato in forma scritta** quando il trattamento riguarda dati sensibili.



Il Consenso (18)

Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici,

I soggetti pubblici non devono richiedere il consenso dell'interessato

Il Consenso (24) Esclusione

Casi nei quali può essere effettuato il trattamento senza consenso

- a) è necessario **per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;**
- b) è necessario **per eseguire obblighi derivanti da un contratto** del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- c) 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;

Il Consenso (24) Esclusione

- d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- e) 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;
- f) 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;

Il Consenso (24) Esclusione

- g) 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, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;
- h) 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;

Il Consenso (24) Esclusione

i) 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;

i-bis) riguarda dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis;

i-ter) con esclusione della diffusione e fatto salvo quanto previsto dall'articolo 130 del presente codice, riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrative contabili, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13.

Informativa (!) e consenso (?)...



La parola all'Avv. Gallus

Misure idonee e misure minime

Misure minime

Cosa sono le misure minime?

Complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 3 l.

Si applicano a tutti i trattamenti di dati (e quindi anche a quelli effettuati senza strumenti elettronici, o qualora venga usato un singolo pc non in rete locale)

La maggior parte delle misure non sono effettivamente “nuove”

Misure idonee e minime

Le “misure minime” sono una creazione del Legislatore italiano

Occorre evitare qualunque confusione tra le due tipologie

Le misure minime sono indicate analiticamente nell'Allegato B

Le misure idonee sono quelle individuate dall'art. 3 l

l'inosservanza delle misure minime è **penalmente sanzionata**,
mentre la mancata adozione delle misure idonee potrebbe
far sorgere una **responsabilità civile**

Misure minime di sicurezza

Per non ingenerare una falsa sensazione di sicurezza, occorre chiarire che

Il pieno rispetto delle misure minime evita sicuramente la responsabilità penale, ma non è idoneo (o può non essere sufficiente) per scongiurare una responsabilità civile da trattamento illecito

Misure minime di sicurezza

- * Trattamenti con o senza l'ausilio di mezzi informatici
- * Sistemi di autenticazione informatica
- * Sistemi di autorizzazione
- * Aggiornamento del software
- * Protezione dagli accessi abusivi o virali
- * Backup sistematici automatizzati
- * [Documento programmatico sulla sicurezza]

Misure minime di sicurezza

Obiettivi da raggiungere con l'adozione delle misure minime di sicurezza:

- 1) Evitare i rischi di perdita o distruzione, anche accidentale, dei dati (integrità)
- 2) Impedire i casi di accesso non autorizzato o di trattamento non consentito di dati (confidenzialità)
- 3) Evitare i casi di accesso abusivo
- 4) Rispettare il principio di continuità del trattamento dei dati

Autenticazione informatica

Quando i dati vengono trattati con strumenti elettronici, occorre subordinare l'accesso degli incaricati al trattamento a una procedura di autenticazione

Le credenziali di autenticazione di solito consistono in userid e corrispettiva password.

L'autenticazione informatica può correttamente espletarsi con usb dongle o anche mediante altri strumenti che utilizzino caratteristiche biometriche (scansione retinica, digitale...) dell'interessato

Autenticazione informatica

In altri termini un essere umano può autenticarsi ad un sistema in tre modi fondamentali:

in base a quello che è:

DNA, impronte digitali, impronta vocale, schema retinico, stile della grafia...

in base a quello che ha:

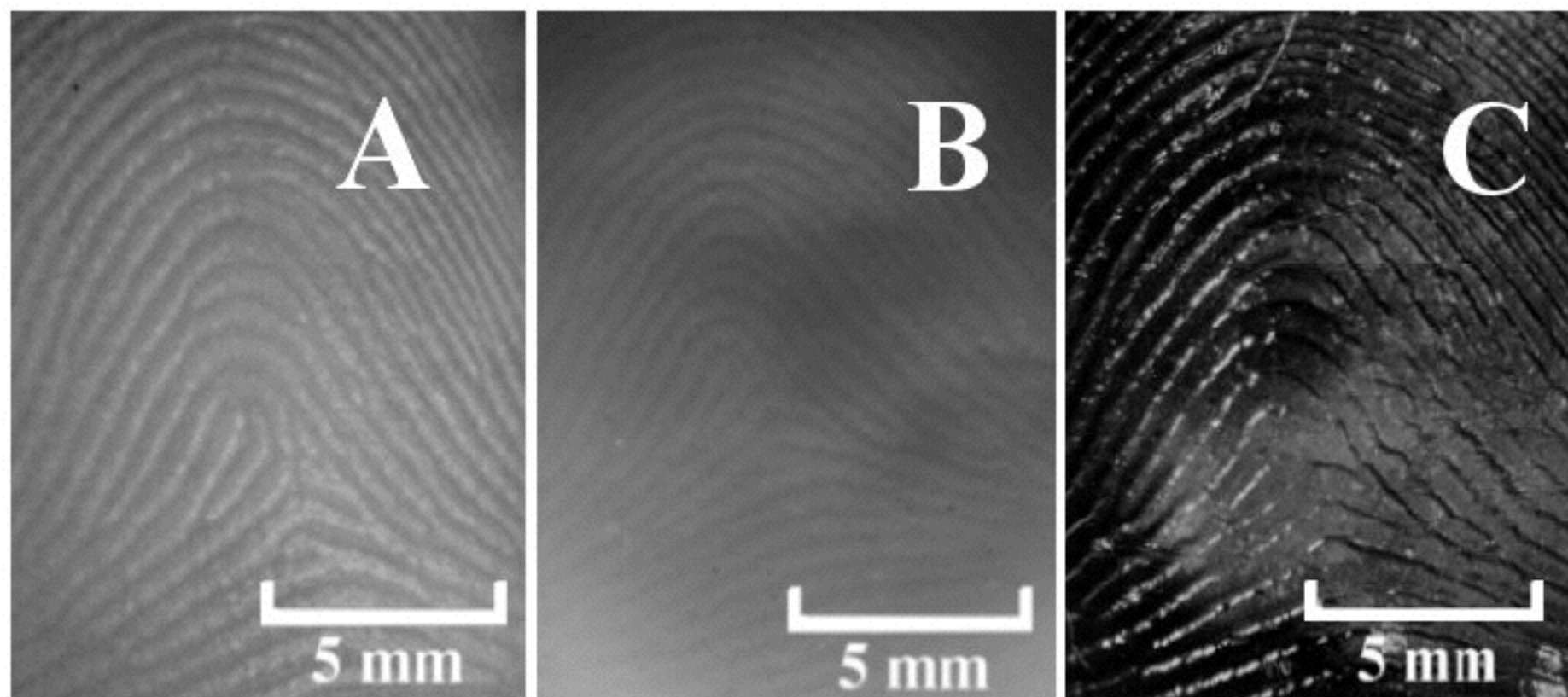
tesserino identificativo, badge, chiave hardware...

in base a quello che conosce:

password, PIN,

Ambiguità dei dati biometrici

Per la maggior parte dei dati biometrici, quelli papillari in testa, si è dimostrato un certo tasso di ambiguità che non dà la certezza del rispetto delle misure idonee allo stato della tecnica.



Incombenze degli incaricati

Gli incaricati cui siano state attribuite delle credenziali di autenticazione informatica sono tenuti a conservare in modo sicuro e riservato la loro password o gli strumenti di identificazione delle caratteristiche biometriche.

Quale password?

Password vietate: quelle che contengano riferimenti agevolmente riconducibili all'incaricato.

Password sconsigliate: quelle costituite da parole contenute in un vocabolario

Le password vanno modificate almeno ogni tre mesi (dati sensibili e giudiziari)

Quale password?

Metodi per creare una buona password:

Tecnica delle “poesie”. Utilizzare e modificare dei testi che sicuramente ricorderemo

Esempio: “Tanto caro mi fu quest'ermo colle”

potrebbe diventare: tacamifuquerco ed ancora..

T^c4m l FuqU3rc0. Questa potrebbe essere una buona password!

Tecnica della generazione automatica mediante sw o siti internet.

Ad esempio: <http://strongpasswordgenerator.com/>

Caratteristiche delle password

La parola chiave dev'essere composta da non meno di 8 caratteri.

Se il sistema non consente l'inserimento di almeno 8 caratteri, la password deve comporsi del numero massimo di caratteri accettati dal sistema.

Lo stesso codice di autenticazione non può essere utilizzato per più di un incaricato, nemmeno in tempi diversi.

Altre disposizioni in tema di credenziali

Le credenziali di autenticazione che non siano utilizzate da almeno 6 mesi sono disattivate, salvo quelle autorizzate per scopi di gestione tecnica degli strumenti informatici

Qualora l'incaricato perda tale qualità, devono essere disattivate anche le credenziali di autenticazione a lui conferite.

Istruzioni agli incaricati

Gli incaricati al trattamento devono essere istruiti sulla gestione delle credenziali di autenticazione, anche in merito alla custodia ed all'inaccessibilità degli strumenti informatici ai terzi non autorizzati al trattamento.

Esempio: screensaver protetto da password, porte chiuse a chiave in caso di brevi assenze degli incaricati dalla postazione di lavoro...

Prolungata assenza o impedimento dell'incaricato

Qualora solo un incaricato abbia accesso a dati ristretti da autenticazione informatica, devono essere impartite idonee e preventive disposizioni scritte con le quali il titolare possa entrare nella disponibilità di dati o strumenti elettronici.

Questo procedimento di recupero dei dati da parte del titolare consente di avere una continuità nel trattamento dei dati anche in caso di prolungata assenza o impedimento dell'incaricato

Il sistema di autorizzazione

Il titolare o il responsabile possono individuare, tra gli incaricati al trattamento diversi gradi di trattamento consentito. In questo caso deve essere apprestato un sistema di autorizzazione.

L'autorizzazione consente di differenziare i privilegi di accesso allo stesso sistema informatico da parte di più soggetti.

Il profilo di autorizzazione può essere creato anche per classi omogenee di soggetti prima dell'inizio del trattamento

Il sistema di autorizzazione

Almeno una volta all'anno è prevista la verifica delle condizioni di autorizzazione in capo a soggetti determinati

Taluni SO non sono in grado di gestire criteri di autorizzazione (windows xp home edition ad esempio). Si può ovviare a tale inconveniente adottando dei sw che creino delle partizioni virtuali criptate

Altre misure “minime” di sicurezza:l'aggiornamento della lista degli incaricati

Oltre alla verifica almeno a cadenza annuale delle autorizzazioni è prevista la verifica della lista degli incaricati e degli addetti alla gestione o alla manutenzione degli strumenti informatici

Altre misure “minime” di sicurezza: l'aggiornamento dell'antivirus

L'all. B prevede, all'art. 16, che i dati siano protetti contro i rischi di intrusione, che verranno più dettagliatamente analizzati nel prosieguo di questa esposizione.

I dati devono, inoltre, essere protetti contro i programmi di cui al 615-quinquies c.p., ossia quelli potenzialmente idonei a danneggiare i sistemi informatici. Questi strumenti, come gli antivirus, devono essere aggiornati almeno ogni sei mesi

Altre misure “minime” di sicurezza: l'aggiornamento di sw e OS

Tutti i programmi e l'intero Sistema Operativo vanno aggiornati periodicamente (a cadenza almeno annuale) al fine di eliminare le vulnerabilità sfruttabili nei modi che vedremo e di correggerne i difetti

Altre misure “minime” di sicurezza: backup settimanale

Almeno una volta alla settimana deve essere eseguito il backup dei dati.

Il backup è un'operazione che permette di conservare i dati (preferibilmente su supporti ottici non riscrivibili) e consente di prevenire inaspettati blocchi del sistema o dannosissime perdite di dati. L'aggiornamento settimanale, tuttavia, potrebbe non bastare. E' sempre consigliabile il backup quotidiano dei dati, anche se fosse soltanto di tipo incrementale su supporti magnetici.

Altre misure “minime” di sicurezza: sw anti intrusione

Le misure ulteriori sono previste in tutti i casi in cui si trattino dati sensibili o giudiziari.

Tali misure minime consistono in strumenti che eliminino o limitino al massimo il pericolo di accesso abusivo a sistema informatico o telematico di cui all'art. 615-ter c.p.

Ulteriori misure di sicurezza in casi particolari

comma 6 art. 22

I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di **cifratura** o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità

Misure di tutela e garanzia

Nell'ambito delle misure di tutela e garanzia di cui sopra si inseriscono determinati soggetti esterni che possono operare mediante contratti di outsourcing mettendo a disposizione del titolare anche strutture proprie. Si pensi, ad esempio, ai tecnici non dipendenti dalla struttura del titolare o società specializzate nella fornitura di servizi di sicurezza informatica.

Misure minime e... idonee

“Si avrà l'esigenza di valutare la idoneità di una misura di sicurezza quando essa sarà stata violata. La sua è una prova diabolica.”

Misure “ulteriori” di sicurezza: custodia e uso dei supporti rimovibili

La cancellazione dei dati attraverso il cestino di windows non garantisce l'effettiva sparizione dei dati dal computer. Occorre usare software specifici per raggiungere risultati apprezzabili

La tecnica usata da tali software (alcuni disponibili gratuitamente in rete come eraser) si chiama wiping e permette la formattazione ripetuta sullo spazio fisico occupato in precedenza dal file.

<http://eraser.heidi.ie>

<http://privacyroot.com/programs/info/italian/wipe.html>

Misure “ulteriori” di sicurezza: misure idonee a recuperare i dati

Devono essere, inoltre, adottate le misure idonee a garantire il pronto ripristino dei dati nel caso di danneggiamento degli stessi o degli strumenti elettronici, entro e non oltre sette giorni

The best way to recover from unexpected data loss is to be properly prepared

La cancellazione accidentale

L'implementazione di un buon sistema di backup dovrebbe essere sufficiente a fronteggiare anche l'eventualità di danni dovuti a cancellazioni accidentali.

Esistono in rete, strumenti gratuiti anche per far fronte a tali eventualità.

Le cancellazioni non eseguite tramite wiping sono, solitamente, recuperabili anche con sw come Recuva (Windows), PhotoRec (Windows/Mac/Linux), Restoration (Windows), “PcInspector File Recovery” (Windows)

Misure di tutela e garanzia

Qualora il titolare si avvalga, per l'adozione delle misure minime di sicurezza di cui all'all. B, di soggetti esterni alla propria struttura, deve ricevere da essi una descrizione scritta degli interventi effettuati unitamente ad un'attestazione della conformità del proprio operato a quanto prescritto dal Disciplinare Tecnico sulle misure minime di sicurezza

La parola all'Avv. Gallus

Gli amministratori di sistema e le norme sulla privacy

Amministratori di sistema

Provvedimento del Garante del 27 novembre 2008

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema

Il provvedimento introduce specifici adempimenti (“misure e accorgimenti”) a carico di **tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici**, esclusi quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili

Casi esclusi

Sono esclusi i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle misure di semplificazione introdotte nel corso del 2008 per legge

(art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 27 novembre 2008).

Finalità

“promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare”

Sys Admin

Chi è l'amministratore di sistema?

- **Figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali**
- **Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software”.**

Sys Admin

Quali sono gli adempimenti?

Obbligo di designazione per **iscritto** da parte del titolare, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'**elencazione analitica degli ambiti di operatività consentiti** in base al profilo di autorizzazione assegnato.

Creazione di un **elenco** degli ADS, contenente le funzioni attribuite, da tenere costantemente aggiornato;

~~[Aggiornamento del DPS, con l'indicazione dell'avvenuta nomina dell'ADS]~~

Adempimenti: valutazione personale

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione **dell'esperienza**, della **capacità** e **dell'affidabilità** del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Non si tratta, però, di valutare la “moralità” del designando sysadmin!

Adempimenti: valutazione personale

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato...

Si devono indicare i singoli sistemi e le singole operazioni affidate?

No. E' sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia ritenuto necessario in casi specifici.

Adempimenti: elenchi sysadmin

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Adempimenti: verifica

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Adempimenti: registrazione degli accessi

Devono essere adottati sistemi idonei alla **registrazione degli accessi logici** (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di **completezza, inalterabilità e possibilità di verifica** della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Adempimenti: registrazione degli accessi

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Gli event records generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento, una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato...).

Chi può essere nominato ADS?

Può essere designato ADS sia un dipendente, che un collaboratore, che un soggetto (persona fisica) esterno, incaricato del trattamento, purché sia in possesso delle caratteristiche di **esperienza, capacità e affidabilità** richieste dal Provvedimento.

La scelta deve essere effettuata tenendo presente che l'ADS deve fornire **idonea garanzia del pieno rispetto** delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla **sicurezza**

Quali adempimenti?

Vanno registrati gli accessi, ed anche i tentativi di accesso e le disconnessioni ai sistemi di elaborazione (non solo al server ma anche ai client) a software e data base

Quanto all'inalterabilità, il Garante ha precisato che “Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software. Il requisito può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili”

Sanzioni?

Quali sanzioni in caso di omessa adozione delle misure riguardanti l'ADS, ove dovute?

Il provvedimento del Garante è stato emanato ai sensi dell'art. 154, lett. C e H del Codice della Privacy

L'art. 162, comma 2-ter. prevede che *“In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da 30.000,00 euro a 180.000,00 euro”*

Q&A

Avv. Francesco Paolo Micozzi



@fpmicozzi