Sistemi informativi: averne fiducia e trarne valore

Capitolo di Milano

AIEA FLASH Gennaio 2010

E' già passato un anno…… Vi ricordiamo che l'iscrizione all'Associazione, anche per l'anno 2010, dovrà essere fatta via web. L'iscrizione via web, avviata l'anno scorso, è stata molto positivamente apprezzata dalla gran parte dei soci e da ISACA.
Sul sito www.aiea.it troverete tutte le istruzioni.
Ricordiamo ai ritardatari che le **iscrizioni** avrebbero dovuto essere fatte **entro e non oltre il 31 dicembre**. Affrettatevi, per non incorrere nelle "sanzioni" ISACA che comportano la cancellazione del socio e la necessità di provvedere ad una iscrizione ex-novo!!!

A proposito di Convegno…..
Sono cominciate le attività preparatorie al prossimo Convegno del 2010. Molto probabilmente, sarà tenuto in una città del centro Italia.
Stiamo già valutando i possibili temi da trattare, sempre facendo riferimento ai temi di Assurance, Security e Governance.
Chi volesse contribuire, segnalando argomenti di particolare interesse, è pregato rivolgersi a aiea@aiea.it, specificando, nell'oggetto "ARGOMENTI DI INTERESSE"

Nuovo tag sul logo ISACA
Isaca ha modificato il proprio logo (lo trovate qui di seguito) ed ha accettato la traduzione proposta da AIEA.

Sistemi informativi: averne fiducia e trarne valore
Milano Chapter

AIEA partecipa
Ricordiamo che AIEA partecipa all'organizzazione del corso dell'Università Statale di Milano sull'IT Governance per promuovere e diffondere l'utilizzo di strumenti di governo dei sistemi informativi aziendali. Il nuovo Corso di Perfezionamento in IT Governance post-laurea, che si terrà nel periodo marzo-giugno 2010 e con iscrizioni entro gennaio 2010, nasce dall'idea di far crescere la figura professionale dell'esperto IT, coniugando la conoscenza delle tecnologie informatiche con le metodologie di gestione dei processi IT e di analisi delle problematiche di efficienza, rischio e misura delle performance.
Per le iscrizioni e per ulteriori informazioni si consulti il sito "itgov.dti.unimi.it".

Il nuovo Consiglio Direttivo
Il 31 dicembre è scaduto il mandato dell'attuale CD e, quindi, sono iniziate le procedure di rinnovo. In questi giorni scade la richiesta di candidature. Raccolte le candidature, si effettuerà, via mail, la procedura di votazione.

I **risultati del Gruppo di Ricerca "ISMS2"**
Il prossimo 27 gennaio, a Roma, saranno presentati i risultati del Gruppo di Ricerca sul tema *"Il knowledge based information security risk management: guida all'eccellenza operativa nel risk management per la sicurezza delle informazioni"* elaborata dal Gruppo di Ricerca sugli ISMS 2.

Il coordinatore del Gruppo, Luigi Carrozzi farà una panoramica delle attività svolte e degli obiettivi raggiunti, lasciando, poi, la parola ad alcuni componenti del Gruppo di Ricerca, i quali illustreranno interessanti aspetti del lavoro svolto, descrivendo il progetto ed i risultati ottenuti.
I risultati del lavoro sono stati pubblicati nella Guida AIEA n.ro 7, che sarà distribuita ai soci presenti. La guida sarà distribuita a Milano e Torino, nelle prossime Sessioni di Studio.

Corsi CISA, CISM, IS Audit base e COBIT

Sono già stati programmati i corsi CISA e CISM, per la preparazione alla sessione del 12 giugno dell'esame, e i corsi di IS Audit base e di COBIT, sia base che avanzato. Le date dei corsi sono disponibili sul sito.

Parlano di noi

Nella Newsletter di dicembre 2009 avevamo dato la notizia
La Newsletter di novembre di CLUSIT parla di noi.
Infatti, nel presentare il programma del Security Summit, che si terrà a Milano dal 16 al 18 marzo 2010, è evidenziato quanto segue:

SESSIONI SULLA GESTIONE DELLA SICUREZZA (in collaborazione con AIEA):

Ora possiamo aggiungere che si sta lavorando per una sessione, il 16 marzo, dalle ore 11.00 alle ore 12.45. La sessione è appartenente al percorso formativo «Gestione della Sicurezza» ed affronterà il tema "Il Ritorno dell'investimento in sicurezza informatica (ROSI)".

In pratica saranno presentati i risultati del GdR sul ROSI, con distribuzione di un quaderno che il gruppo sta scrivendo. Alla sessione parteciperanno: AIEA, Clusit, Oracle, Deloitte e KPMG (le 3 aziende sono anche sponsor del Summit).
Per AIEA, parteciperà Alberto Piamonte, che è attivo nel GdR come rappresentante AIEA

Il programma del Security Summit prevede, inoltre, che:

saranno presentati i risultati del Gruppo di Ricerca AIEA che sono stati pubblicato nella Guida AIEA n.4 *COBIT 4.1 e ISO27001 confronto Quantitativo e Qualitativo*

saranno brevemente illustrati gli obiettivi del costituendo gruppo di Ricerca in fase di attivazione insieme a itSMF sul confronto COBIT con ITIL

AIEA parteciperà, insieme a CLUSIT e ACFE al percorso formativo «Gestione della Sicurezza» sul tema « Frodi Interne ».

Gruppi di Lavoro / Ricerca

"Traduzione Cobit 4.1"

Informiamo i soci che nell'Area Download del sito si trovano:

l'"Executive Summary",

tutti i processi dei domini:

- Pianificazione ed Organizzazione,
- Acquisizione e Realizzazione,
- Erogazione ed Assistenza,
- Monitoraggio e Valutazione.

L'introduzione, con il framework, sarà completata entro gennaio 2010.

COBIT e legge 262

Il Gruppo di Ricerca AIEA è articolato in 6 sottogruppi chiamati Focus Group.
I partecipanti alla ricerca sono ben 17 soci divisi in 6 Focus Group i cui Relatori sono:
Alessandro Arca (FG5)
Giuliano Flesia (FG4)
Luca Nurisso (FG1 e FG6)
Dino Ponghetti (FG3)
Luca Turri (FG2)

Le tematiche dei Focus Group sono le seguenti:

FG1: Introduzione e normativa di riferimento
FG2: Dimensionamento delle verifiche e analisi dei rischi
FG3: Controlli generali
FG4: Controlli applicativi
FG5: Campionamenti
FG6: Valutazione del sistema di controllo e attestazioni finali

La conclusione di tutte le attività è prevista a breve.

Gruppo di Lavoro "Traduzione Val IT 2.0"

Con il coordinamento di Guido Leone, il Gruppo di Lavoro si è occupato della traduzione della versione aggiornata di Val IT 2.0. In particolare delle seguenti pubblicazioni:

Enterprise Value:Governance of IT Investments - The Business Case
Enterprise Value: Governance of IT Investments - Getting Started with Value Management
Enterprise Value: Governance of IT Investments - The Val IT Framework 2.0
Sono stati rilasciati, in occasione del convegno di Pisa, i primi due documenti.

Dopo il rilascio, in occasione del convegno di Pisa, dei primi due documenti, ora è terminata la traduzione del terzo ("The Val IT Framework 2.0").
Il lavoro è terminato ed è stata attivata la fase di pubblicazione di questa **nuova Guida AIEA** che conterrà i risultati del Gruppo di Lavoro e che, nei prossimi mesi, sarà distribuita ai soci.
Al Gruppo hanno partecipato 17 soci.

Gruppo di Lavoro ROSI (RETURN ON SECURITY INVESTMENT)

Lo scorso mese di settembre si è costituito un Gruppo di Lavoro sul ROSI (GdL), su iniziativa di AIEA, Clusit e Oracle, con la partecipazione di Deloitte, Ernst & Young, KPMG e PriceWaterhouseCoopers. Il GdL sta lavorando alla preparazione di un quaderno/studio che contenga indicazioni utili per le aziende per il calcolo del ROSI all'inteno dei propri progetti di sicurezza. Non si pretende di ottenere uno strumento preciso, ma almeno una serie di indicazioni sulla metodologia da utilizzare e sui fattori da prendere in considerazione per calcolare il ROSI. Lo studio sarà presentato a marzo 2010 nel corso del Security Summit di Milano.

Sistemi informativi: averne fiducia e trarne valore

Capitolo di Milano

I prossimi eventi di AIEA

Calendario Eventi AIEA

Gennaio 2010

27…..……..Lugano –Sessione di Studio
27…..……..Roma – Sessione di Studio

Febbraio 2010

9…..……..Milano – Inizio corso COBIT
17…..…..……..Milano – Sessione di Studio
18…..……....Torino – Sessione di Studio

ATTENZIONE.
Sulla Home page del sito www.aiea.it è disponibile il calendario di tutti gli eventi programmati da AIEA nell'anno 2010

Sistemi informativi: averne fiducia e trarne valore

Capitolo di Milano

I prossimi eventi ISACA:

Calendar of Events

Dates of conferences/events are indicated in RED; other dates and deadlines are indicated in BLACK.

January

13 January.....Early-bird deadline for EuroCACS, Budapest, Hungary
15 January.....Deadline for 2010 membership and certification renewals
20 January.....Deadline for contributions to volume

February

10 February .....Early-bird deadline for North America CACS, Chicago, Illinois, USA
22-23 February.....**Asia-Pacific CACS**SM, Mumbai, India
25 February .....Deadline for ISACA volunteer applications

Avviso ai soci 1
Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo, azienda di appartenenza o altro…) di comunicare i nuovi dati in segreteria **aiea@aiea.it**. La mancanza di tali comunicazioni potrebbero impedire, al socio, la ricezione delle comunicazioni.

Avviso ai soci 2
E' in linea, sulla homepage del sito, il calendario degli eventi AIEA.
Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2009 sia nelle Sessioni di Studio sia in Workshop.
Chi volesse dare il proprio contributo, è pregato inviare una mail a aiea@aiea.it, specificando, nell'oggetto "ARGOMENTI DI INTERESSE"
In una successiva newsletter provvederemo ad elencare tutti i temi proposti.

Partecipazione di soci ad eventi
Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da segnalare ad esempio nella newsletter.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIEA. La partecipazione dell'Associazione ad un evento "deve" però essere decisa dal Consiglio Direttivo: siete quindi pregati di contattare il CD con ragionevole anticipo!
In caso non fosse possibile la partecipazione a nome AIEA, vi invitiamo ad indicare, nel profilo professionale la vostra appartenenza ad AIEA, Capitolo di ISACA

Bibliografia
E' on line il nuovo numero di InterLex (http://www.interlex.it)

Vi informiamo che sul sito www.cnipa.it sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo che alla stesura di numerosi documenti hanno partecipato diversi nostri soci e che inoltre CNIPA organizza incontri o seminari aperti anche ai soci AIEA.

Le Newsletter delle altre Associazioni

E' disponibile on line, la **Newsletter CLUSIT** del 31 dicembre 2009 (disponibile in PDF all'indirizzo www.clusit.IT/newsletter_31 12_09.pdf))

- Sono disponibili e qui allegate le Newsletter n.ro 343 e 344 del Garante Privacy

E' disponibile on line, la **Newsletter ANSSAIF** all'indirizzo www.anssaif.it

- E' disponibile on line, la **Newsletter AIPSI** all'indirizzo www.aipsi.org/newsletter

Newsletter
NOTIZIARIO SETTIMANALE
ANNO XI
WWW.GARANTEPRIVACY.IT

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NUMERO 332

10 DICEMBRE 2009

- NO AL TELEMARKETING CON NUMERI CASUALI
- RISCOSSIONE: MAGGIORI GARANZIE PER I CONTRIBUENTI
- VIGILANZA PIÙ "VIGILATA" NEGLI AEROPORTI

No al telemarketing con numeri casuali

E' vietato effettuare telefonare commerciali usando sistemi che generano numerazioni casuali. Tanto più se gli abbonati vengono contattati con chiamate preregistrate.
Lo ha stabilito il Garante privacy intervenendo contro una azienda vinicola a seguito delle segnalazioni di numerosi cittadini che lamentavano la ricezione di telefonate indesiderate, in alcuni casi preregistrate. Per le sue comunicazioni commerciali l'azienda non utilizzava, né direttamente né attraverso i propri call center, i numeri presi dagli elenchi telefonici, ma si serviva di un sistema che generava i numeri da contattare attraverso sequenze casuali. Le sequenze erano elaborate con criteri geografici e i numeri non erano abbinati a dati anagrafici.
Nel suo provvedimento di divieto (relatore Giuseppe Fortunato) l'Autorità ha spiegato che anche il numero casualmente composto e chiamato telefonicamente deve considerarsi "dato personale", in quanto ricollegabile, anche indirettamente, a una persona identificata o identificabile. Di conseguenza, in base alle norme sulla privacy, per poter utilizzare anche questo tipo di numerazione a fini commerciali è necessario il previo consenso dell'interessato. Tanto più laddove si utilizzino modalità di contatto con chiamate preregistrate per le quali il consenso è obbligatorio, come più volte ribadito dal Garante.
Accertata l'illiceità del trattamento, il Garante ha vietato all'azienda di usare sistemi che generano tramite digitazione casuale numeri di telefono con i quali contattare gli interessati. La società dovrà inoltre cancellare tutti i dati personali per i quali non risulta documentato tale consenso.
La mancata osservanza del provvedimento del Garante espone a sanzioni penali (reclusione da tre mesi a due anni) e amministrative (pagamento di una somma da trentamila a centottantamila euro).

Riscossione: maggiori garanzie per i contribuenti

Prosegue l'azione del Garante privacy per la messa in sicurezza del sistema informativo del fisco. Sotto la lente il servizio di riscossione a mezzo ruolo, attualmente in fase di riorganizzazione a seguito di profonde modifiche introdotte da una importante riforma di settore che ha riportato la gestione della riscossione in capo all'Amministrazione finanziaria. L'Autorità ha chiesto ad Agenzia delle Entrate, a Equitalia e alle società del gruppo Equitalia maggiori garanzie per i contribuenti, informazioni più chiare sull'uso dei dati personali, adozione di elevate misure di sicurezza, utilizzo di informazioni indispensabili e aggiornate.
Le prescrizioni dell'Autorità tengono conto dei risultati di accertamenti ispettivi che hanno riguardato, oltre agli accessi all'anagrafe tributaria da parte degli agenti della riscossione, anche problematiche più generali del servizio. Agenzia delle entrate, Equitalia e le società partecipate dovranno definire, entro e non oltre i termini indicati dal Garante, le diverse competenze e responsabilità rispetto al trattamento dei dati. Ciò consentirà anche un più agevole esercizio dei diritti da parte dei contribuenti che potranno così individuare con più facilità i destinatari cui rivolgere le loro istanze (accesso, rettifica, cancellazione dei dati ecc.).
Un'informativa semplice e chiara che indichi, tra l'altro, le rispettive competenze sul trattamento dei dati dovrà comunque essere inserita nell'avviso o nella cartella esattoriale inviata al contribuente. Agenzia delle entrate ed Equitalia dovranno, inoltre, rivedere l'articolazione delle diverse banche dati, superando le attuali sovrapposizioni che derivano dalla precedente ripartizione sul territorio del servizio della riscossione, evitando rischi per la correttezza dei dati. Nel sistema informativo dovranno essere contenuti dati il più possibile esatti, aggiornati e pertinenti, conservati per periodi di tempo stabiliti a seconda delle esigenze.
Agenzia delle entrate dovrà, infine, garantire elevate misure di sicurezza e predisporre procedure di controllo interno sugli accessi effettuati a fine di riscossione

all'anagrafe tributaria, con particolare riguardo all'anagrafe dei rapporti bancari. Ciò anche in relazione agli accessi effettuati dagli enti locali, tramite società esterne, al fine di reperire informazioni per la riscossione delle proprie entrate. Analoghi controlli dovranno essere predisposti da Equitalia sulle attività svolte dalle società del gruppo e da Sogei.
Prescrizioni analoghe sono state impartite dal Garante alla Regione Siciliana e alle società che si occupano della riscossione nell'isola.

Vigilanza più "vigilata" negli aeroporti

Accessi alle aeree riservate con le impronte digitali

Il Garante per la protezione dei dati personali ha autorizzato una società, che svolge attività di vigilanza e sicurezza aeroportuale, a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti di Milano "Linate" e "Malpensa", Roma "Fiumicino", Venezia e Pisa.
L'azienda aveva sottoposto alla verifica preliminare del Garante un progetto che prevedeva la possibilità di rilevare con il sistema biometrico la presenza dei lavoratori. Il progetto escludeva comunque il controllo sull'orario di lavoro.
L'esigenza della società era quella di scongiurare accessi indebiti nelle cosiddette "aree sterili" (security restricted area*)* degli aeroporti, ovvero nelle zone preposte ai controlli pre-volo dei passeggeri, dei bagagli a mano e da stiva, delle merci e degli operatori aeroportuali di staff.
Per tali aree il "Programma Nazionale di Sicurezza" prevede non solo limitazioni di accesso, ma anche particolari misure di sicurezza necessarie per prevenire, ad esempio,
l'introduzione a bordo degli aeromobili di armi, ordigni esplosivi e qualsiasi altro oggetto pericoloso.
Il sistema biometrico contenuto nel progetto si basa sul confronto tra le impronte digitali rilevate e il template (la rappresentazione in codice numerico), memorizzato e cifrato su una smart card nell'esclusiva disponibilità del lavoratore, che ha prestato preventivamente il proprio specifico consenso al trattamento dei dati.
L'Autorità (con un provvedimento di cui è stato relatore Mauro Paissan) ha ritenuto proporzionati la raccolta e l'uso delle impronte digitali dei dipendenti in relazione agli accessi alle sole "aree sterili". Ha tuttavia prescritto alla società di prevedere modalità alternative di accesso e identificazione e di fornire ai dipendenti un'apposita informativa che indichi la natura facoltativa del consenso al trattamento dei dati biometrici. I dati relativi agli accessi alle "aree sterili" potranno essere conservati per un tempo massimo di sette giorni.

L'attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Privacy e Social Network: la guida del Garante privacy in distribuzione gratuita presso i principali uffici postali italiani – Comunicato del 20.11.2009

Video asilo di Pistoia: il Garante richiama i media, oscurate i volti dei bambini – Comunicato del 4.12.2009

NEWSLETTER
del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. *Newsletter* è consultabile sul sito Internet www.garanteprivacy.it

Newsletter
NOTIZIARIO SETTIMANALE
ANNO XI
WWW.GARANTEPRIVACY.IT

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NUMERO 333

11 GENNAIO 2010

- ILLECITE ALCUNE FOTO DI GEORGE CLOONEY
- NO A RACCOLTE INDISCRIMINATE SULL'HIV NEGLI STUDI MEDICI
- SFRUTTAMENTO ILLECITO DELL'IMMAGINE: STOP DEL GARANTE

Illecite alcune foto di George Clooney

Non si possono scattare e diffondere fotografie, anche di personaggi famosi, violando la riservatezza di dimore private protette alla vista esterna. Nessun problema, invece, riguardo a foto scattate in luoghi visibili al pubblico.
Lo ha stabilito il Garante, con un provvedimento di cui è stato relatore Mauro Paissan, rispondendo alla segnalazione dell'attore George Clooney che lamentava la pubblicazione, da parte di alcune testate giornalistiche, di immagini che lo ritraevano con alcuni ospiti all'interno del parco della sua villa.
Alcune fotografie oggetto della segnalazione mostrano persone che si trovavano all'interno del giardino della villa, in zone circondate da un'alta siepe o da un muro di cinta che impediscono ai passanti la vista. Dagli accertamenti del Garante è emerso che tali immagini sono state raccolte con espedienti (ad esempio, aprendo dei varchi nella siepe), violando così la ragionevole aspettativa di intimità e riservatezza creata dalla barriera visiva posta a protezione della dimora privata. Le modalità con cui sono state acquisite queste immagini - ha sottolineato l'Autorità - contrastano con quelle garanzie di trasparenza e di correttezza che devono caratterizzare la raccolta di dati personali a cui si devono attenere i giornalisti nell'esercizio della loro attività, indipendentemente dalla notorietà dei personaggi coinvolti.
Altre fotografie, invece, sono state scattate in luoghi normalmente visibili dall'esterno, ad esempio, presso la scalinata di accesso alla villa, o l'affaccio di un balcone. In questo caso, l'Autorità ha ritenuto leciti gli scatti, in quanto ritraggono le persone in luoghi pubblici o, comunque, aperti al pubblico, oppure in aree "per loro natura esposte alla visibilità da parte di terzi".
Il Garante ha dunque vietato il trattamento e l'ulteriore diffusione delle immagini raccolte in modo illegittimo e ha altresì prescritto alle tre testate giornalistiche, alle agenzie e ai fotografi coinvolti di informare sugli esiti del provvedimento tutti coloro ai quali sono state eventualmente cedute le fotografie sottoposte a divieto.

No a raccolte indiscriminate sull'Hiv negli studi medici

Coloro che esercitano la professione sanitaria non devono raccogliere informazioni sulla sieropositività di ogni paziente che si rivolge per la prima volta allo studio medico, se ciò non è indispensabile per il tipo di intervento o terapia che deve eseguire. Il dato sull'infezione da Hiv può essere raccolto dal medico, infatti, solo qualora sia ritenuto necessario in relazione all'intervento clinico da eseguire sul paziente e comunque con il suo consenso.
Lo ha stabilito il Garante privacy con un provvedimento generale in cui ha indicato i principi ai quali devono attenersi i medici nella raccolta di informazioni sulla sieropositività. Il Garante ha sentito la necessità di fornire indicazioni a tutti gli studi medici dopo aver affrontato il caso di uno studio dentistico che raccoglieva informazioni sull'Hiv mediante la distribuzione di un questionario al momento dell'accettazione dei pazienti. Allo studio è stato vietato l'uso dei dati raccolti. Alla base dell'intervento del Garante c'è, dunque, lo stop ad una raccolta generalizzata e ingiustificata di informazioni delicatissime.
Nel primo colloquio con il paziente - ha spiegato l'Autorità - una volta acquisito il consenso al trattamento dei dati personali, il medico deve raccogliere solo le informazioni sanitarie necessarie ad assicurare una corretta assistenza medica. L'esigenza di raccogliere informazioni sull'Hiv fin dal momento dell'accettazione - continua l'Autorità - non può essere giustificata neanche dalla necessità di attivare specifiche misure di protezione per il contagio, poiché la normativa di settore prevede che tali misure siano adottate, nei confronti di ogni paziente, a prescindere dalla conoscenza dello stato di sieropositività.
Il Garante ha precisato, infine, che nel caso in cui il medico venga a conoscenza di un caso di Aids o di Hiv, oltre a rispettare specifici obblighi di segretezza e non discriminazione nei confronti del pazienze, ha l'obbligo di adottare ogni misura individuata dal Codice privacy per garantire la sicurezza dei dati sanitari.

Sfruttamento illecito dell'immagine: stop del Garante

Non è possibile sfruttare commercialmente l'immagine di una persona, anche se nota, senza il suo consenso.
Lo ha stabilito il Garante affrontando il caso di una donna di spettacolo, impegnata anche in politica, che aveva casualmente scoperto la sua fotografia su alcuni volantini pubblicitari utilizzati per reclamizzare servizi odontoiatrici. L'interessata aveva diffidato il centro dentistico dal proseguire il volantinaggio ma, dopo aver scoperto che le pubblicità erano ancora in distribuzione presso una delle sedi dello studio, aveva chiesto l'intervento del Garante.
Dagli accertamenti avviati dall'Autorità è emerso che lo studio professionale aveva scaricato la fotografia della donna da un sito web e, senza il consenso dell'interessata, l'aveva poi stampata su 50.000 volantini.
L'Autorità - anche sulla base di quanto stabilito dalla disciplina sul diritto d'autore - ha sottolineato che la riproduzione e la divulgazione del ritratto di una persona nota senza il suo consenso, anche nel caso in cui si tratta di un'immagine liberamente reperibile su internet, è lecita soltanto se risponde a esigenze di "pubblica informazione" e non ad altre finalità, in particolare quelle commerciali.
Essendo stati violati i principi di liceità e correttezza fissati dal Codice privacy, il Garante ha dunque vietato allo studio dentistico l'ulteriore trattamento, in qualunque forma, della foto della donna, inclusa la distribuzione, presso le diverse sedi, dei volantini già stampati.
L'Autorità ha, inoltre, avviato un autonomo procedimento per l'eventuale contestazione delle sanzioni amministrative relative alle violazioni alla normativa sulla privacy commesse dallo studio dentistico.

L'attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Amministratori di sistema: precisazioni del Garante - Comunicato del 10.12.2009

Analisi mediche via mail. Le regole del Garante privacy - Comunicato del 21.12.2009

Rinnovate le autorizzazioni generali per i dati sensibili e giudiziari - Comunicato del 29.12.2009

Telemarketing: riconfermate le regole del Garante privacy - Comunicato del 30.12.2009

NEWSLETTER
del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. *Newsletter* è consultabile sul sito Internet www.garanteprivacy.it