Paolo Giardini
STUDIO GIARDINI
Eucip Certified Informatics Professional
Consulente per la sicurezza delle informazioni
AIP – OPSI – AIPSI – CLUSIT - ISSA - FORMEZ - ILS

Le nuove disposizioni in materia di Privacy

Camucia 13/03/2009

OPSI - AIP

- OPSI - Osservatorio Privacy e Sicurezza Informatica nasce in seno all'Associazione Informatici Professionisti.
- Ha come scopo lo studio delle problematiche relative alla Sicurezza informatica ed ai rischi legati alla tutela dei dati personali e confidenziali.
- Promuove la cultura della Sicurezza Informatica.
- Si propone come centro di concertazione e di confronto tra le varie associazioni, gruppi e aziende pubbliche e private che si occupano di sicurezza.
- Rappresenta AIP presso il Garante Privacy al tavolo per la redazione del Codice Deontologico per i servizi di telecomunicazione.

Agenda

- Le semplificazioni amministrative
- Le nuove disposizioni per il DPS
- Le misure di sicurezza
- I supporti informatici
- Amministratori di sistema
- Sanzioni
- Conclusioni

Le semplificazioni degli adempimenti rispetto ai trattamenti per finalità amministrative e contabili

Il provvedimento

Nell'ottica dei principi di semplificazione, armonizzazione ed efficacia indicati dall'art.2 del "Codice in materia di protezione dei dati personali" (D.lgs 196/2003) il Garante ha emesso il 19 giugno 2008 un nuovo provvedimento per la semplificazione degli adempimenti connessi al trattamento di dati personali effettuati da aziende, enti pubblici e professionisti (gazzetta ufficiale del 1 luglio 2008).

Le semplificazioni

Sono previste una serie di semplificazioni in relazione ad informativa, consenso, nomina degli incaricati

- La semplificazione è relativa ai dati trattati per l'ordinaria attività di gestione amministrativa e contabile nei casi in cui non siano trattati dati di carattere sensibile e giudiziario.
- Non si tratta di novità in quanto viene ripreso e rafforzato quanto già espresso in precedenti provvedimenti, snellendo quanto previsto dal Codice stesso.

Informativa

Può essere resa anche solo oralmente una unica informativa per tutti i trattamenti effettuati quando questi siano richiesti a seguito di obblighi contrattuali, precontrattuali o normativi ed anche per lo svolgimento di correnti finalità amministrative e contabili.

L'informativa dovrà essere resa in linguaggio semplice e comprensibile (non in "burocratichese"), fornendo all'interessato le informazioni essenziali e rimandando per il testo completo ad un sito web.

Un esempio

A tale proposito il Garante suggerisce la seguente formulazione per moduli, fatture, ecc.:

"I SUOI DATI PERSONALI.

Utilizziamo - anche tramite collaboratori esterni - i dati che la riguardano esclusivamente per nostre finalità amministrative e contabili, anche quando li comunichiamo a terzi. Informazioni dettagliate, anche in ordine al suo diritto di accesso e agli altri suoi diritti, sono riportate su..."

Suggerimenti

Il Garante suggerisce di utilizzare gli spazi riservati alle note nelle comunicazioni commerciali (fatture, offerte ed altri documenti) per riportare l'informativa proposta. Dovranno essere predisposti in tal caso strumenti per permettere agli interessati di avere tutte le informazioni aggiornate sui trattamenti effettuati.

Ad esempio l'informativa completa potrà essere pubblicata sul sito web, su bacheche, cartelli esposti al pubblico, ecc.

E' necessario in questi casi che sia prevista la data dell'ultimo aggiornamento dell'informativa.

Quando semplificare

La semplificazione dell'informativa riguarda anche tutti i dati già noti all'interessato. Ad esempio gli estremi del titolare quando questi possono essere rilevati in altra parte del documento (intestazione, carta intestata).

E' invece necessaria una informativa specifica per quei trattamenti che prevedano ulteriori forme oltre alle ordinarie esigenze amministrative e contabili, ad esempio la raccolta di dati per finalità di marketing.

Consenso

Il consenso, come specificato dall'art. 24 del Codice, non è richiesto nella maggior parte dei trattamenti normalmente effettuati dalle aziende: ad esempio per eseguire obblighi derivanti da contratto del quale è parte l'interessato, quando i dati trattati siano provenienti da pubblici registri o qualora i dati trattati riguardino lo svolgimento di attività economiche, compresi i rapporti precontrattuali (trattative, offerte...).

Altre semplificazioni

- La designazione degli incaricati può essere fatta evitando singoli documenti per ciascun incaricato ma mediante un unico documento riportate le caratteristiche e le modalità dei trattamenti effettuati da ciascuna unità, sempre che sia documentata l'appartenenza a detta unità dei singoli incaricati.
- La notifica va fatta solo nei casi indicati dall'art. 37 del codice, ovvero per i trattamenti relativi a dati genetici, telelocalizzazione, ecc.
- Il d.l. 112 (del 25 giugno 2008) semplifica ulteriormente le modalità di notificazione che dovrà essere effettuata tramite il sito web del Garante.

Attività post vendita

- le aziende che abbiano venduto un bene o fornito un servizio possono utilizzare i dati del cliente per l'invio sia cartaceo che via email di materiale pubblicitario nonché la possibilità di utilizzare i dati dei clienti per ricerche di mercato,
- deve trattarsi di prodotti analoghi a quelli forniti in precedenza
- l'interessato, debitamente informato, al momento della raccolta dei dati o successivamente può opporsi, nel rispetto delle garanzie in materia di profilazione degli interessati (provvedimento 245 febbraio 2005).
- E' comunque obbligatorio fornire in ogni comunicazione la possibilità di opt-out, ovvero di negare il consenso al trattamento in maniera semplice (fax, telefono, email) e inviando in tal caso all'interessato la conferma dell'interruzione del trattamento.

Cosa fare

- Semplificare il processo attraverso un'unica informativa privacy anziché molteplici informative, senza ripetizioni o frammentazioni della stessa come invece avveniva per i singoli aspetti del rapporto con gli interessati.
- Produrre meno carta e meno burocrazia attraverso l'utilizzo di informative sintetiche riportate nella fattura e negli ordini, nei siti aziendali, nelle bacheche, nelle segreterie telefoniche, ricordando di inserire l'indicazione dell'ultimo aggiornamento, sfruttando la possibilità di nomina semplificata per gli incaricati ed evitando di richiedere il consenso se non necessario.

L'esonero dalla redazione del DPS

Il testo dell'art.29 L.133/2008

“Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato documento programmatico sulla sicurezza e' sostituita dall'obbligo di autocertificazione resa dal titolare del trattamento (...) di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte.”

Cosa dice la norma

Questa norma si applica esclusivamente a chi effettua trattamenti di dati non sensibili e che trattano come unico dato sensibile quello legato allo stato di salute dei dipendenti e collaboratori (con esclusione della diagnosi) o quello relativo all'adesione ad organizzazioni sindacali od a carattere sindacale, effettuato per fini legati alla gestione amministrativa e contabile.

Chi rientra nei casi previsti può sostituire il DPS con una autocertificazione

Cosa è l'autocertificazione

- L'autocertificazione è uno strumento previsto dall'art. 47 del DPR 445 del 28 dicembre 2000
- Consiste nella facoltà riconosciuta ai cittadini di presentare, in sostituzione delle tradizionali certificazioni richieste, propri stati e requisiti personali, mediante apposite dichiarazioni sottoscritte (firmate) dall'interessato. La firma non deve essere autenticata.
- L'autocertificazione sostituisce i certificati senza che ci sia necessità di presentare successivamente il certificato vero e proprio. La pubblica amministrazione ha l'obbligo di accettarle, riservandosi la possibilità di controllo e verifica in caso di sussistenza di ragionevoli dubbi sulla veridicità del loro contenuto.

Cosa fare

Se il trattamento effettuato rientra nei casi indicati per l'esenzione dalla redazione del DPS si dovrà provvedere a redarre una autocertificazione, ai sensi dell'art. 47 DPR 28 dicembre 2000, n. 445.

L'autocertificazione, ovvero *dichiarazione sostitutiva dell'atto di notorietà* dovrà essere redatta e firmata dal Titolare del trattamento (quindi non da un responsabile) il quale sotto la propria responsabilità penale certifica la rispondenza dei trattamenti effettuati a quanto stabilito dalla normativa, in particolare per quanto riguarda le misure di sicurezza minime ed idonee.

Dubbi legittimi...

Quale è la reale portata del provvedimento?

A chi si applica?

Quali sono le eventuali sanzioni?

Ad esempio, il trattamento di dati dei dipendenti relativi a razza o religione o orientamento politico non è compreso pertanto resta l'obbligo di redazione del DPS, così come per il trattamento di dati giudiziari.

Si veda il caso di dipendenti con incarichi politici e relativa gestione permessi, o nel caso di assunzioni di dipendenti o collaboratori mussulmani, ebrei, testimoni di Geova, con le relative esigenze dettate dal credo religioso, dati sensibili relativi a parenti di dipendenti (p.e. assistenza diversamente abili), ecc...

Altri casi

Altri esempi di casi nei quali sussiste l'obbligo di redazione del DPS sono:

- Trattamento di dati personali a fini di marketing e profilazione
- Utilizzo di caratteristiche biometriche (p.e. per accesso ai locali)
- Installazione di sistemi di geolocalizzazione (p.e. antifurto veicoli)
- ed in generale per ogni trattamento di dati sensibili o giudiziari che esuli da quelli previsti, ovvero “stato di salute o malattia” e “adesione ad organizzazioni sindacali o a carattere sindacale”

Cosa si rischia

L'autocertificazione, al pari del DPS e delle altre misure previste dall'art. 34, è una misura minima di sicurezza, la cui inosservanza prevede fino a 2 anni di carcere e multe fino a 50.000 euro (art. 169).

In caso di falsa dichiarazione si commette reato ai sensi dell'art. 168 del D.lgs 196/2003 (falsità nelle dichiarazioni al Garante) punibile con la reclusione da 6 mesi a 3 anni.

Falsa dichiarazione

Inoltre la falsità in atti (ad esempio produrre un documento che attesta il falso durante un'ispezione) viene punita dal c.p.

- - Falsa attestazione di fatti in atto pubblico art.483 C.P.: reclusione fino a 2 anni
  - Uso di atto falso art.489 C.P.: reclusione fino a 1 anno e 4 mesi
  - Dichiarazione mendace resa al pubblico ufficiale in atto pubblico: reclusione fino a 3 anni (Art.495 C.P.: dichiarare il falso direttamente in un atto pubblico o in una dichiarazione destinata a esservi riprodotta, dinanzi al pubblico ufficiale, relativamente all'identità, allo stato o a qualità personali proprie o di altri).

DPS o autocertificazione?

Posso fare a meno del DPS?

Forse. Sicuramente non posso fare a meno delle misure di sicurezza richieste dalla normativa.

E' quindi necessario effettuare una analisi corretta ed approfondita dei dati trattati, delle modalità di trattamento e dei rischi correlati per evitare di incorrere in sanzioni, allo stesso tempo snellire e semplificare gli adempimenti e aumentando produttività, sicurezza dei dati e continuità aziendale.

Sarà a partire dai risultati di questa analisi che si potranno definire ed approntare i documenti richiesti (regolamento internet, informative, DPS od autocertificazione) e le necessarie misure di sicurezza.

Quindi?

Siamo davvero certi di non trattare in nessun modo (ricordate la definizione di trattamento?) un dato sensibile?

Se abbiamo questa **certezza**, ok. Niente DPS.

Ma per avere questa certezza è necessario effettuare una analisi approfondita dei dati e dei trattamenti, quindi...

DPS Semplificato

Il Provvedimento del 27/11/2008 prevede la possibilità di redarre un DPS semplificato per i titolari che trattano "*dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso professionisti, artigiani e piccole e medie imprese*"

Cosa è richiesto

- le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento;
- una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;
- l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità;
- una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

DPS Semplificato

La semplificazione riduce la portata del DPS da manuale del “Sistema gestione Privacy” a semplice documento riepilogativo.

Ad esempio non è necessario formalizzare l'analisi dei rischi o le modalità di disaster recovery

DPS Semplificato

Si deve fare però attenzione perché in realtà, una analisi viene richiesta dal provvedimento quando si prescrive "*una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate…*"

DPS: riepilogo

- DPS completo: trattamento dati sensibili con strumenti elettronici
- DPS ridotto: trattamento dati sensibili per finalità amministrative e contabili (solo PMI, artigiani, professionisti)
- Autocertificazione: nessun trattamento dati sensibili

Le misure di sicurezza

provvedimento 27/11/2008

Semplificazioni: per chi

- le semplificazioni riguardano i Titolari che trattano "*soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale*"
- PMI , artigiani, professionisti che *trattano dati personali anche sensibili solo per finalità amministrative e contabili*

Quali semplificazioni

- Istruzioni agli incaricati: possono essere impartite anche verbalmente. (*Come dimostro in caso di necessità di avere ottemperato agli obblighi?)*
- Autenticazione e autorizzazione: si possono adottare i sistemi di login del sistema operativo. Svaniscono gli obblighi relativi a lunghezza, scadenza, ecc. delle password. (*Come mi difendo da una richiesta di risarcimento a norma dell'art. 2050 c.c.?*)
- Backup: mensile
- Aggiornamenti dei software (p.e. antivirus); annuale
- Obbligo di verifica periodica

Trattamenti cartacei

- La semplificazione riguarda soprattutto la possibilità di impartire istruzioni orali.
- Non è necessario identificare chi accede agli archivi al di furori dell'orario di lavoro.

I supporti informatici

provvedimento 13/10/2008

Le problematiche

Il Garante Privacy ha preso in considerazione una serie di problematiche di sicurezza per i dati personali legate ai supporti informatici nel provvedimento del 13/10/2008

Prevenire la diffusione di dati personali a causa di:

- Furto di notebook
- Smarrimento di chiavette usb
- Dismissione di hard disk, Cdrom, DVD, computer
- Riutilizzo di hardware dismesso

Furto o smarrimento

- Proteggere i dati personali tramite sistemi di cifratura, del file, gruppo di file o del file system

Riutilizzo di hardware

- Cancellazione sicura dei dati personali tramite sovrascrittura ripetuta più volte (da 7 a 35) mediante appositi strumenti software

Nb: gli esperti concordano che una sola sovrascrittura impedisce di fatto la rilettura dei dati

Smaltimento

- Distruzione fisica dei supporti
- Cd e dvd anche con distruggi documenti
- Hard disk anche con demagnetizzazione

Documentare le attività

- Chi reimpiega materiale dismesso deve accertarsi che non contenga dati personali; nel caso deve acquisire autorizzazione alla loro distruzione
- Chi effettua operazioni di distruzione o cancellazione dei dati deve redarre attestazione dell'attività svolta

Amministratori di sistema

Il provvedimento

Il provvedimento del Garante Privacy del 27/11/2008, (g.u. 24/12/2008) prevede per gli amministratori di sistema una serie di obblighi, pur rendendo finalmente giustizia ad una figura professionale fin'ora negletta.

Chi è interessato

Il provvedimento non riguarda coloro che rientrano nelle semplificazioni esaminate.

Pertanto, i Titolari che effettuano trattamenti con strumenti elettronici "*soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale*" sono esentati

Amministratori di sistema

Con questo termine il Garante intende non solo “il tecnico incaricato della gestione del sistema informatico” ma in senso molto più ampio anche tutti coloro che per le loro funzioni possono od hanno la possibilità di accedere ai dati personali.

Quindi, si va dal tecnico che accede al pc per cambiare il mouse, al gestore di database, all'addetto al backup, al webmaster...

Obblighi Amministrativi

Il Titolare deve effettuare la nomina ad amministratore di sistema "*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 della sicurezza*".

La nomina è individuale.

Valutazione

Il Titolare deve effettuare almeno annualmente una valutazione dell'operato dell'amministratore di sistema per verificarne la rispondenza “alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.”

Elenco amministratori

Il Titolare deve redigere un elenco nominativo degli amministratori e dei rispettivi compiti.

L'elenco deve comprendere i nominativi di eventuali incaricati esterni (outsourcing)

Questo elenco deve essere inserito nel DPS o in caso di esenzione in un documento da conservare per eventuali ispezioni.

Registrazione accessi

Gli accessi (login) ai sistemi di elaborazione ed agli archivi elettronici effettuati dagli amministratori di sistema devono essere registrati con modalità che abbiano "*caratteristiche di completezza, in alterabilità e possibilità di verifica della loro integrità*".

Le registrazioni debbono comprendere data e ora e la descrizione dell'evento che le ha generate.

La registrazione deve essere conservata per almeno 6 mesi.

Entrata in vigore

Entro il 30 giugno 2009, come per le norme relative alla “strong authentication” per gli incaricati che accedono ai dati di traffico nell'ambito dell'attività di call center

Sanzioni

Le nuove sanzioni

In generale sono state ritoccate tutte le sanzioni portandole al doppio degli importi precedenti (art. 44 DL 207/2008, gazzetta ufficiale del 31/12/2008 n. 304).

Si riportano due casi a titolo di esempio.

Omissione misure di sicurezza

In caso di violazione delle norme sulle misure di sicurezza si applica una sanzione amministrativa da 20.000 a 120.000 euro senza pagamento in misura ridotta ed una pena di 2 anni di carcere.

Il reato si estingue se si opera un “ravvedimento operoso” entro un periodo di tempo fissato (max 6 mesi) con il pagamento di una ammenda pari ad un quarto del massimo della sanzione *(oltre alla sanzione)*

Non adeguamento provv. Amministratori

L'Art. 162 comma 2 ter, inosservanza dei provvedimenti del garante,è un illecito amministrativo, prevede la sanzione amministrativa da 30000 a 120000 euro, "in ogni caso".

Definizioni

Definizione PMI

Dal decreto del 18 aprile 2005 Ministero delle Attività Produttive (raccomandazione della Commissione europea 2003/361/CE del 6 maggio 2003) di definiscono PMI le imprese che hanno:

* meno di 250 occupati

* un fatturato annuo non superiore a 50 milioni di euro, oppure un totale di bilancio annuo non superiore a 43 milioni di euro.

* sono piccole imprese quelle che hanno meno di 50 occupati e un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro

* sono microimprese quelle che hanno meno di 10 occupati e un fatturato annuo oppure un totale di bilancio annuo non superiore a 2 milioni di euro

Correnti finalità amministrative e contabili

Finalità amministrative: organizzazione aziendale; tenuta contatti con soggetti interni ed esterni; gestione personale; adempimenti PA

Finalità contabili: tutti gli adempimenti relativi alla tenuta della contabilità a fini civilistici e fiscali; rapporti con banche ed altri soggetti di natura finanziaria

Approfondimenti

Si rimanda al documento OPSI OD09.001 "Quadro riepilogativo delle normative sulla Privacy emanate nel 2008"

Per ulteriori approfondimenti si consiglia di consultare il sito del Garante Privacy

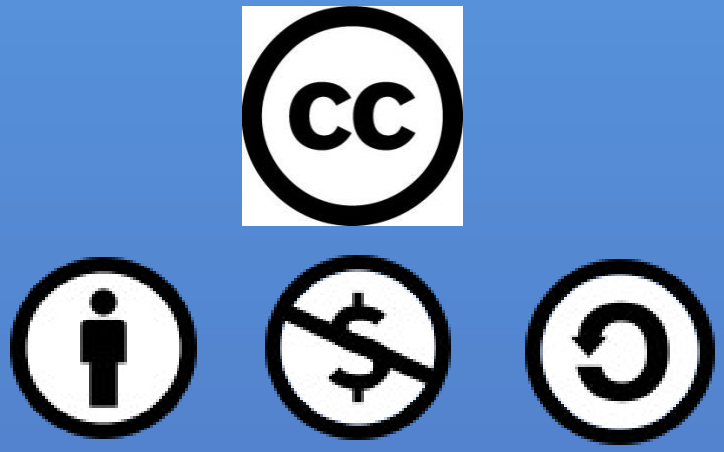
Grazie per l'attenzione

paolo.giardini@aipnet.it

http://blog.solution.it

Questo lavoro viene distribuito sotto licenza

Creative Commons 3.0



Sei libero di copiare, distribuire, trasmettere quest'opera e di modificarla a condizione di: attribuirne la paternità all'autore originale, non usare quest'opera per fini commerciali, condividerla allo stesso modo.