Incontro di approfondimento

PQA
Progetto Qualità e Ambiente

Logica&

LogiConsulting s.r.l
SOFTWARE HARDWARE INTERNET SOLUTION

AMMINISTRATORI DI SISTEMA:

LE NUOVE PRESCRIZIONI PRIVACY PER I TITOLARI DEL TRATTAMENTO

Mantova, 16-11-2009

Hotel La Favorita

Progetto Qualità e Ambiente S.n.c., Via Parigi 38, 46047 Porto Mantovano (MN), www.pqa.it, info@pqa.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Focus sul Codice Privacy

- Chi è tenuto all'applicazione del Codice Privacy
- Quali sono i principali adempimenti obbligatori
- Quali sono stati i provvedimenti del Garante più significativi dalla data di entrata in vigore del Codice Privacy ad oggi

Chi è tenuto all'applicazione del Codice Privacy

- Il Codice Privacy si applica a "*chiunque tratti dati personali … per finalità non personali*" (clienti, dipendenti, fornitori, utenti, cittadini, pazienti, colleghi, soci, associati, ecc...)

- Quindi, sono interessati all'adeguamento:
  - tutte le imprese operanti del settore privato
  - gli studi professionali
  - le pubbliche amministrazioni come comuni, ospedali, scuole, istituti universitari, ecc..
  - le associazioni
  - le cooperative

Parliamo lo stesso linguaggio: alcune definizioni utili

Le principali parole chiave sulle quali è necessario dare un’esatta definizione sono:

Trattamento

Dati Personali

Alcune definizioni dei termini più utilizzati

Trattamento (di dati)

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti:

la raccolta	il raffronto
la registrazione	l'utilizzo
l'organizzazione	l'interconnessione
la conservazione	il blocco
la consultazione	la comunicazione
l'elaborazione	la diffusione
la modificazione	la cancellazione
la selezione	la distruzione di dati
l'estrazione	

Alcune definizioni dei termini più utilizzati

Dati Personali

Sensibili

Dati idonei a rilevare l'origine razziale, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni, od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale

Giudiziari

Dati idonei a rilevare provvedimenti in materia di casellario giudiziale, di anagrafe di sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o indagato

I principali adempimenti obbligatori

- Redazione **delle informative** Privacy (clienti, fornitori, dipendenti, sito internet, curricula, videosoveglianza, ecc.)
- Individuazione della **tipologia di trattamenti effettuati**
- Nomina dei **responsabili del trattamento** (facoltativa)
- Nomina degli **incaricati al trattamento**
- Individuazione ed implementazione delle **misure minime di sicurezza** (elettroniche e cartacee)
- Redazione di un **Regolamento Interno** per l'utilizzo delle risorse informatiche (internet - email)
- Redazione del **Documento Programmatico sulla Sicurezza**
- **Formazione** degli incaricati al trattamento dei dati

I provvedimenti più significativi emanati dal Garante Privacy fino ad oggi

mar/2007	Linee guida per posta elettronica e internet
mar/2008	Tutela della salute e sicurezza nei luoghi di lavoro
apr/2008	Limiti al controllo sulla posta elettronica del dipendente
nov/2008	Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice Privacy
nov/2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
dic/2008	Marketing via e-mail: possibile inviare comunicazioni a carattere pubblicitario solo con il consenso preventivo dell'interessato

Le semplificazione delle misure di sicurezza sono applicabili a piccole e medie imprese che trattano dati solo per fini amministrativi e contabili

Le semplificazioni possono così essere riassunte:

- Istruzioni in materia di misure minime di sicurezza – anche solo orali ma espresse chiaramente;
- Modalità di creazione password libera (non è più richiesto un numero minimo di caratteri);
- Aggiornamento programmi antivirus – almeno 1 volta l'anno (ogni 2 anni per pc off–line);
- Back up dei dati – almeno 1 volta al mese;
- Accesso agli archivi cartacei dopo orario ufficio – istruzioni preventive agli incaricati;
- Redazione DPS "semplificato" o autocertificazione.

I provvedimenti più significativi emanati dal Garante Privacy fino ad oggi

mar/2007	Linee guida per posta elettronica e internet
mar/2008	Tutela della salute e sicurezza nei luoghi di lavoro
apr/2008	Limiti al controllo sulla posta elettronica del dipendente
nov/2008	Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice Privacy
nov/2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
dic/2008	Marketing via e-mail: possibile inviare comunicazioni a carattere pubblicitario solo con il consenso preventivo dell'interessato

Incontro di approfondimento

PQA
Progetto Qualità e Ambiente

Logica&

LogiConsulting s.r.l
SOFTWARE HARDWARE INTERNET SOLUTION

AMMINISTRATORI DI SISTEMA:

LE NUOVE PRESCRIZIONI PRIVACY PER I TITOLARI DEL TRATTAMENTO

Mantova, 16-11-2009

Hotel La Favorita

Progetto Qualità e Ambiente S.n.c., Via Parigi 38, 46047 Porto Mantovano (MN), www.pqa.it, info@pqa.it

Provvedimento del Garante in materia di Amministratori di sistema

Con il provvedimento del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), viene richiesto di provvedere entro i termini di scadenza previsti:

1. **di predisporre lettere di incarico e lista degli "amministratori di sistema" per i trattamenti iniziati dopo il 25 gennaio 2009 (attività che verrà completata nei termini di legge previsti per il 30 giugno 2009);**

2. **di richiedere alle società terze a cui sono affidati in outsourcing i trattamenti di dati personali la lista degli amministratori di sistema" che gestiscono tali trattamenti e l'attestazione (per iscritto) che tali "amministratori" hanno le caratteristiche richieste dalla legge;**

3. **di comunicare a tutto il personale (previa comunicazione via email e intranet): contenuti del provvedimento del Garante l'elenco degli amministratori di sistema**

4. **di predisporre un "piano formativo" ad hoc per gli "amministratori di sistema";**

5. **di predisporre un sistema di log per gli accessi effettuati dagli "amministratori di sistema".**

Provvedimento del Garante in materia di Amministratori di sistema

Elementi del Provvedimento	Dettaglio	Note
Amministratore di sistema	I preposti alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti	Le funzioni tipiche dell'amministratore di un sistema sono richiamate nell'Allegato B del codice, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati), alla custodia delle credenziali , alla gestione dei sistemi di autenticazione ed autorizzazione.
	Amministratore di basi dati	
	Amministratori di reti	
	Amministratori di apparati di sicurezza	
	Amministratori di sistemi sw complessi	
Trattamento dati da parte dell'amministratore	Allorquando esista un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali (anche quando l'amministratore non consulti "in chiaro" le informazioni personali)	

Provvedimento del Garante in materia di Amministratori di sistema

Elementi del Provvedimento	Dettaglio	Note
Destinatari	Tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi ed alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema	
Conseguenze	Responsabilità, di ordine penale civile (artt 15 e 169 del Codice), che possono derivare in caso di incauta e inidonea designazione	
Tempistica	Entro il 30 giugno 2009 tutti i titolari di trattamenti in corso al momento della pubblicazione del provvedimento ovvero iniziati entro 30 giorni dalla pubblicazione del provvedimento in Gazzetta Ufficiale (24 dicembre 2008)	
	Tutti i titolari che intraprendano un trattamento di dati decorsi 30 giorni dalla pubblicazione in Gazzetta del provvedimento in oggetto dovranno adottare le misure indicate, anteriormente all'inizio del trattamento stesso	

Provvedimento del Garante in materia di Amministratori di sistema

Misure	Dettagli	Note
Attribuzione funzione del ruolo di "Amministratore di sistema"	L'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione dell'esperienza, della capacità e della'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.	Anche quando le funzioni di amministratore di sistema o assimilate sono attribuibile solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il Titolare ed il Responsabile devono comunque attenersi a criteri di valutazione equipollenti a quelli richiesti per la designazione dei Responsabili ai sensi dell'art. 29
Designazioni individuali	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.	
Elencazione amministratori di sistema	Nel DPS o in un Documento interno devono essere annotati gli estremi identificativi degli "amministratori di sistema"	
	Se i dati trattati riguardano informazioni personali dei lavoratori, i titolari sono tenuti a renderlo noto a questi e a rendere noto l'ambito di operatività	Per fare questo si può inserire questa informazione nell'informativa (ex. Art. 13 del Codice Privacy) mediante il disciplinare tecnico ex Provv. N. 13 del 1 marzo 2007 ovvero mediante altri strumenti di comunicazione interna (intranet, circolari, ordini di servizio …)

Provvedimento del Garante in materia di Amministratori di sistema

Misure	Dettagli		Note
Verifica attività degli amministratori di sistema (cadenza annuale)	Verifica annuale circa la rispondenza dell'operato alle misure organizzative, tecniche, di sicurezza previste dalla normativa vigente		
Registrazione accessi	Registrazione accessi logici da parte degli amministratori. La registrazione deve rispondere a determinate caratteristiche	Completezza	Ciò di fatto significa che i log (relativi all'attività di amministratore) non possono essere memorizzati sul sistema stesso dove sta operando l'amministratore ma debbono essere memorizzati su un "sistema terzo" (immediatamente inviati ad un server esterno), marcati temporalmente, firmati digitalmente (è un ipotesi per certificare la provenienza) e archiviati in modo inalterabile (ad esempio attraverso un sistema di cifratura)
		Inalterabilità	
		Verifica di integrità	
	Contenuto della registrazione	Riferimenti temporali	
		Descrizione evento che le ha generate	
	Retention	Conservazione per almeno 6 mesi	

Tutti i titolari di dati sono obbligati ad applicare le misure previste?

- No, soltanto quelli che trattano dati personali con strumenti informatici ed elettronici, anche quando tale trattamento è parziale.
- Tuttavia anche i titolari che trattano dati in questo modo sono **esclusi** se le finalità del trattamento sono soltanto quelle **amministrativo-contabili** (oggetto dei recenti interventi di semplificazione).

Quali figure rientrano nel concetto di amministratore di sistema?

- Quelle in possesso di competenze tali da poter essere incaricate della gestione e manutenzione dei sistemi informatici o delle loro componenti (hardware e software).
- Nella stessa definizione rientrano anche le figure equiparate che svolgono una attività di gestione e manutenzione che presenta dei rischi relativi alla protezione dei dati personali (amministratori di database, di rete, di sicurezza, di software, ecc...).

Come deve comportarsi il titolare prima di nominare uno o più amministratori di sistema?

- Innanzitutto, può sembrare banale, ma è opportuno verificare se la nomina risponde ad una esigenza effettiva.
- In secondo luogo occorre valutare l'**idoneità** a ricoprire l'incarico da parte del soggetto da designare.
  I criteri per compiere questa valutazione possono essere diversi, ma il garante richiama espressamente quelli previsti per la nomina del **responsabile** del trattamento.

Come deve comportarsi il titolare prima di nominare uno o più amministratori di sistema?

- Questo vuol dire quindi che l'esperienza, la capacità e l'affidabilità del soggetto da designare devono costituire una **garanzia** del rispetto delle disposizioni del codice della privacy, compreso l'aspetto attinente la sicurezza dei dati.
- Se questa valutazione manca o avviene in modo superficiale si può anche incorrere in una **responsabilità** per incauta designazione nel caso in cui il soggetto designato non sia poi in grado di garantire, nei limiti delle proprie funzioni, il livello di protezione dei dati che è lecito attendersi.

Con quali modalità deve avvenire la nomina?

- E' opportuno che sia documentata e che contenga una indicazione precisa delle funzioni e dei compiti attribuiti all'amministratore (così come avviene per il responsabile del trattamento).
- In questo modo si fa chiarezza sull'ambito di esigibilità della prestazione professionale richiesta all'amministratore di sistema.

Che cosa si intende per verifica dell'operato degli amministratori?

- Significa che gli amministratori devono rispettare, nello svolgimento delle attività, le misure tecniche, organizzative e di sicurezza previste dalla legge in materia di protezione dei dati personali e che le eventuali violazioni od anomalie nel loro operato devono essere prontamente identificate e sanate dal titolare.
- Questo garantisce che il titolare possa considerarsi diligente nell'effettuazione dei controlli e spiega il perchè venga richiesto agli amministratori, all'atto della nomina, di fornire idonea garanzia di rispetto delle disposizioni di legge vigenti.

Quando deve essere effettuata la verifica dell'operato degli amministratori?

- Quando si reputa opportuna, anche in relazione alle dimensioni ed alla complessità dell'organizzazione di riferimento e, comunque, con cadenza almeno **annuale**.

L’attività degli amministratori di sistema deve essere registrata?

- Soltanto quella che comporta un **accesso,** inteso come superamento di una procedura di autenticazione informatica, ai sistemi ed agli archivi elettronici.
- In assenza di contrarie indicazioni sembra che la registrazione debba comprendere tanto gli eventi positivi (success) che negativi (failure) di accesso.

Con quali modalità e garanzie deve essere effettuata la registrazione?

- Le registrazioni (record) devono contenere l'indicazione della data (*timestamp*) e la descrizione dell'evento che le genera.
- Devono inoltre essere complete, non modificabili e consentire la verifica della loro integrità, tenendo conto delle finalità di controllo cui sono preordinate.

Con quali modalità e garanzie deve essere effettuata la registrazione?

- A seconda della dimensione e della complessità della infrastruttura IT questa misura può richiedere uno sforzo organizzativo e tecnologico non indifferente, anche dal punto di vista dell'analisi della situazione di partenza.
- Le registrazioni vanno conservate per un periodo minimo di **6 mesi**.

Quanto tempo hanno i titolari per applicare le misure?

- Se i trattamenti sono già iniziati il termine massimo per adempiere è stato prorogato al **15 Dicembre 2009**.
- Se invece i trattamenti devono ancora iniziare le misure devono essere applicate subito.
- E' comunque consigliabile non attendere l'ultimo minuto e pianificare, invece, anche economicamente, l'attuazione delle misure per tempo.

L’amministratore di sistema non è semplicemente il manutentore

della struttura informatica ma è

il “garante informatico”

della protezione delle informazioni personali unitamente al titolare.

Sanzioni

In base alle nuove sanzioni introdotte dal D.L. n.207/08, la violazione amministrativa derivante dall'inosservanza dei provvedimenti di prescrizione delle misure necessarie o di divieto di cui, rispettivamente all'art.154, c.1, lett.c) e d) del D.Lgs. n.196/03 (Codice Privacy) prevede la sanzione consistente nel pagamento di una somma da **€ 30.000 a € 180.000**.

Nei casi di violazioni di minore gravità, l'art.164-bis del D.Lgs. n.196/03, avuto riguardo anche alla natura economica e sociale dell'attività svolta, i limiti minimi e massimi delle sanzioni sono applicati in misura pari a 2/5 (pertanto, nel caso in esame da **€ 12.000 a € 72.000**).

Incontro di approfondimento

PQA
Progetto Qualità e Ambiente

Logica&

LogiConsulting s.r.l
SOFTWARE HARDWARE INTERNET SOLUTION

AMMINISTRATORI DI SISTEMA:

LE NUOVE PRESCRIZIONI PRIVACY PER I TITOLARI DEL TRATTAMENTO

Mantova, 16-11-2009

Hotel La Favorita

Progetto Qualità e Ambiente S.n.c., Via Parigi 38, 46047 Porto Mantovano (MN), www.pqa.it, info@pqa.it

Spazio alle domande!

(15 min.)

GRAZIE DELL'ATTENZIONE