



Trento, 28 gennaio 2009
GF/et
CIRCOLARE N° 5/2009 - S

Agli Enti Soci
- LL.SS. -

OGGETTO: *La figura degli Amministratori di sistema: ruolo chiave per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Le regole del Garante per la protezione dei dati personali.*

Riportiamo di seguito la circolare elaborata dal dott. Gianni Festi, dello sportello di consulenza in materia di privacy, dello scrivente Consorzio dei Comuni Trentini.

Si segnala, con l'avvertenza di prestare la dovuta attenzione, l'adozione da parte del Garante per la protezione dei dati personali, del recente provvedimento generale di data 27 novembre 2007 (pubblicato nella Gazzetta Ufficiale n. 300 del 24 dicembre 2008) avente ad oggetto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

I titolari di trattamenti di dati personali e quindi anche gli enti locali sono tenuti a seguire le prescrizioni e ad adottare alcune misure, come di seguito illustrate.

Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche, chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati di cui sono titolari gli enti.

La loro individuazione e designazione riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, sono essenziali per la sicurezza dei trattamenti svolti.

Si rammenta che i titolari di trattamenti sono tenuti, ai sensi dell'art. 31 del Codice, ad adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti e che per la loro mancata o non idonea adozione assumono responsabilità penale, amministrativa e civile (al riguardo si veda la recente circolare in merito all'inasprimento delle sanzioni)

Chi è l'Amministratore di sistema?

L'"amministratore di sistema" è il soggetto cui è affidata la gestione e la manutenzione di un impianto di elaborazione o di sue componenti o, in generale, del sistema informatico. Sono però anche considerati tali altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi.



Gli amministratori di sistema, pur non dovendo trattare dati personali (e quindi anche conoscerli) per l'esercizio delle loro funzioni, svolgono spesso specifiche attività che comportano elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware* comportano in molti casi un'effettiva capacità di conoscenza e azione su informazioni; ciò comporta a tutti gli effetti trattamento di dati personali, anche quando, ad esempio, l'amministratore non consulti "in chiaro" le informazioni medesime.

Misure e accorgimenti da adottare

1. Valutazione delle caratteristiche soggettive

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.

2. Designazione individuale

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica dei compiti e delle funzioni assegnati nonché degli ambiti di operatività consentiti.

3. Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza. Inoltre, se l'attività degli amministratori di sistema riguarda anche servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, deve essere resa nota o conoscibile agli stessi l'identità degli amministratori di sistema. Ciò mediante l'inserimento di tale informazione nell'informativa resa ai lavoratori ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro, oppure tramite il disciplinare tecnico sull'uso di internet e della posta elettronica o, in alternativa, mediante strumenti di comunicazione interna (a es., *intranet* aziendale, ordini di servizio a circolazione interna o bollettini).

4. Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari 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.

5. 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.

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.

Tempi di adozione delle misure e degli accorgimenti

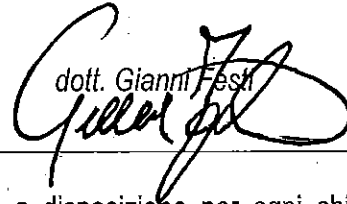
Le misure e gli accorgimenti devono essere adottati entro e non oltre il **24 aprile 2009**.

Quali sono le possibili sanzioni?

Per l'inosservanza delle prescrizioni o mancata adozione delle misure è prevista la sanzione amministrativa del pagamento di una **somma da € 30.000 a € 180.000**, ai sensi dell'art. 161 comma 2 ter del Codice.



Lo Sportello Privacy è a disposizione per qualsiasi chiarimento o approfondimento relativo al provvedimento.

dott. Gianni Festi


Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.

Cordiali saluti.

Il Direttore
dott. Alessandro Ceschi


Il Presidente
dott. Marino Simoni
