

## Gestori di Rete, come ti rinomino un fantasma.

E' di questi giorni una iniziativa dell'Agenzia delle Entrate-Direzione Centrale Audit e Sicurezza-Settore Sicurezza-Ufficio Normative Speciali, prot. n° 2009/188135 del giorno 11/12/2009: "**Direttiva per la designazione dei soggetti che svolgono le funzioni di amministratori di sistema nelle strutture dell'Agenzia delle Entrate**".

Tale documento è stato inviato alle Direzioni regionali il **14/12/2009** e da queste agli Uffici Locali il successivo **15/12/2009**, raccomandandone l'urgenza poiché gli adempimenti richiesti avevano scadenza nello stesso giorno **15/12/2009**. (!)

### Perchè tanta sollecitudine?

E' una questione che parte da lontano, da un provvedimento del **27/11/2008** dell'Autorità Garante per la protezione dei dati personali volto ad assicurare protezione dei dati durante il loro trattamento da parte di enti pubblici ed organismi privati.

Il Provvedimento stabiliva come termine entro il quale assicurare adempimento delle prescrizioni il **30/06/2009**.

Qualche mese dopo l'emanazione, la citata Autorità Garante proponeva a maggio 2009 dal sito internet istituzionale una consultazione pubblica dei soggetti interessati (i titolari del trattamento) con cui chiedeva espressamente di ricevere osservazioni.

Tant'è che in data **25/06/2009** l'Autorità, tenuto conto delle segnalazioni pervenute circa problematiche soprattutto tecniche per l'attuazione delle misure di adeguamento richieste (che devono essere soprattutto onerose in termini monetari e di organizzazione), firma un provvedimento di proroga dei termini fino al **15/12/2009**.

Insomma, nel frattempo e nel complesso, molte aziende private e pubbliche, piccole e grandi, cominciando a ragionare su quanto veniva richiesto, si sono rese conto che effettivamente c'erano molte cose da ristabilire negli **incarichi di lavoro (soprattutto in quelle realtà lavorative dove l'attività di AdS è affidata in outsourcing, cioè a soggetti esterni)**: se il fine del provvedimento è invitare i titolari di trattamenti ad adottare particolari cautele ed a riflettere con la dovuta attenzione nella fase di individuazione e scelta degli amministratori di sistema (AdS), il Garante ha raggiunto in parte l'obiettivo.

L'Autorità espone una attenta **analisi delle problematiche**:

**RILEVATA l'esigenza** di intraprendere una specifica attività rispetto ai soggetti preposti ad attività riconducibili alle mansioni tipiche dei c.d. "amministratori di sistema", nonché di coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati, evidenziandone la rilevanza rispetto ai trattamenti di dati personali anche allo scopo di promuovere presso i relativi titolari e nel pubblico la consapevolezza della delicatezza di tali peculiari mansioni nella "Società dell'informazione" e dei rischi a esse associati;

**CONSIDERATA l'esigenza** di consentire più agevolmente, nei dovuti casi, la conoscibilità dell'esistenza di tali figure o di ruoli analoghi svolti in relazione a talune fasi del trattamento all'interno di enti e organizzazioni;

**RITENUTA la necessità** di 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 (due diligence);

**CONSTATATO** che lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti;

**RILEVATA la necessità** di richiamare l'attenzione su tale rischio del pubblico, nonché di persone giuridiche, pubbliche amministrazioni e di altri enti (di seguito sinteticamente individuati con l'espressione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice) che impiegano, in riferimento alla gestione di banche dati o reti informatiche, sistemi di elaborazione utilizzati da una molteplicità di incaricati con diverse funzioni, applicative o sistemistiche;

**RILEVATO** che i titolari sono tenuti, ai sensi dell'art. 31 del Codice, ad adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (artt. 15 e 169 del Codice);

**CONSTATATO** che l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti;

**CONSIDERATO** inoltre che, qualora ritenga facoltativamente di designare uno o più responsabili del trattamento, il titolare è tenuto a individuare solo soggetti che "per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza" (art. 29, comma 2, del Codice);

**RITENUTO** che i titolari di alcuni trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati e sono stati pertanto oggetto di recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Prov. Garante 6 novembre 2008), debbano essere allo stato esclusi dall'ambito applicativo del presente provvedimento.

Quindi, come recepito dalla Direttiva **dell'Agenzia delle Entrate**, "**prescrive ai titolari**, da un lato, l'adozione di **idonee cautele** nell'individuazione dei soggetti deputati allo

svolgimento delle funzioni di amministratore di sistema e nell'introduzione di apposite **regole** per lo svolgimento delle loro mansioni, e dall'altro, l'impiego di **accorgimenti** e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare (due diligence), al fine di prevenire ed accertare eventuali accessi non consentiti ai dati personali da parte degli amministratori di sistema, in specie quelli realizzati con **abuso** della loro qualità.

L'Agenzia, in quanto titolare dei trattamenti di dati personali dei contribuenti e dei propri dipendenti presenti nella banca dati dell'Anagrafe tributaria e negli applicativi impiegati nei processi lavorativi, è tenuta ad applicare il provvedimento in esame.

Il presente documento presenta, pertanto, una disamina degli aspetti salienti del provvedimento del Garante e fornisce le linee guida necessarie per dare attuazione, nell'ambito delle strutture centrali e periferiche dell'Agenzia, agli adempimenti in esso previsti, con particolare riguardo alla designazione degli amministratori di sistema.

La presente direttiva dovrà trovare applicazione nell'intera struttura organizzativa dell'Agenzia, ovvero presso le Direzioni Centrali e Regionali, e tutte le Direzioni Provinciali, gli uffici periferici, i centri di assistenza multicanale, i centri operativi ed i centri satellite.

Per le strutture periferiche dell'Agenzia, con il richiamato provvedimento il Direttore ha designato quali responsabili operativi i direttori degli uffici locali e delle altre strutture omologhe (centri di assistenza multicanale, centri operativi e centri satellite).

Con riferimento alle direzioni provinciali già attive ed a quelle che saranno attivate, è da intendersi quale responsabile operativo, ai sensi del citato atto del 30 gennaio, il Direttore Provinciale.

Pertanto, nelle ipotesi in cui gli adempimenti di cui alla presente direttiva siano posti in essere dai direttori degli uffici locali, a seguito della successiva convergenza dell'ufficio nella direzione provinciale, sarà cura del nuovo Direttore provinciale provvedere nuovamente agli adempimenti ivi previsti.

Il provvedimento concerne le figure di "amministratore di sistema", intendendo per tali non solo quelle che, in ambito informatico, sono "finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti", ma anche "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".

L'individuazione dei soggetti coinvolti risulta abbastanza problematica, soprattutto in assenza di una definizione normativa e/o tecnica condivisa dell'amministratore di sistema. In sostanza essi devono essere individuati, nell'ambito dell'Agenzia, tra i soggetti che, poiché sono funzionalmente deputati allo svolgimento di 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, hanno, per ciò stesso, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò **anche quando questi non consultino "in chiaro" le informazioni medesime.** **(che vuol dire: anche se le informazioni sono criptate, nulla esclude che il fantasma di turno -ipotesi- possa farsene una copia da decriptare poi con calma)**

La prescrizione dell'Agenzia delle Entrate si conclude con le seguenti note:

Al soggetto designato sono fornite per iscritto le **istruzioni** previste dalla legge, che si allegano al presente atto di cui fanno parte integrante.

Alle predette istruzioni l'amministratore dovrà attenersi scrupolosamente tenuto conto dello specifico ruolo al quale sono preposti.

L'amministratore riceve dal titolare **idonea formazione** sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

Ebbene negli Uffici dove è stato designato l'AdS sembra non siano state fornite le previste istruzioni, ma ancor di più la formazione (organizzeranno dei corsi dopo?).

Ciò che preoccupa è la **responsabilità** del provvedimento, l'AdS non ne è destinatario, ma soggiace agli effetti che ne scaturiranno con rilevanza anche **penale**: "La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante.

Ci si riferisce, in particolare, all'**abuso** della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di **frode informatica** (art. 640 ter), nonché per le fattispecie di **danneggiamento** di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinquies) di recente modifica."

Le pene relative agli articoli del Codice Penale citati sono:

- ex art. 615 ter: da 1 a 5 anni di reclusione o da 3 a 8 anni (a seconda della gravità);
- ex art. 640 ter: da 6 mesi a 3 anni di reclusione oltre a sanzione pecuniaria da Lire 100.000 a Lire 2.000.000 o da 1 a 5 anni oltre a sanzione pecuniaria da Lire 600.000 a Lire 3.000.000 (a seconda della gravità);
- ex art. 635 bis: da 6 mesi a 3 anni di reclusione o da 1 a 4 anni (a seconda della gravità);
- ex art. 635 ter: da 1 a 4 anni di reclusione o da 3 a 8 anni (a seconda della gravità);
- ex art. 635 quater: da 1 a 5 anni di reclusione;
- ex art. 635 quinquies: da 1 a a anni di reclusione;

Mentre per i **Titolari del trattamento** dei dati, destinatari del provvedimento e responsabili della nomina degli AdS sono previste le sanzioni di cui all'art.169 del DLGS 30/06/2003, n. 196 dal titolo "Codice in materia di protezione dei dati personali" (**l'arresto sino a due anni o l'ammenda da diecimila euro a cinquantamila euro**).

Solo che questo ultimo articolo dice che "1. Chiunque, essendovi tenuto, omette di adottare le **misure minime** previste dall'articolo 33 e' punito con ...", quindi la mancata o la errata individuazione e nomina dell'AdS è una misura minima, così' minima che...

...**non adeguando la politica degli accessi ai sistemi**, in caso di indagine, come potrà un Gestore di Rete, ancorché Amministratore di Sistema, dimostrare di non essere stato lui a compiere determinati atti in un **apparato vulnerabile e gestito da un soggetto esterno** come quello esistente?

- le credenziali amministrative di accesso ai server sono identiche, da anni, per tutti gli uffici;
- in caso di coesistenza di due o più Gestori di Rete che condividono le stesse credenziali amministrative di accesso per i client, chi sarà stato a fare la tale cosa?
- Non viene tracciato l'accesso remoto ai sistemi sia client che server;
- Come possono i Gestori di Rete assumersi la responsabilità di cose di cui non hanno il controllo? Allo stato attuale anche i GdiR sono utilizzatori di un'architettura gestita da altri.

Se questo voleva essere il preludio ad una **seria riorganizzazione e "messa in sicurezza" dell'apparato**, gli interventi sono intempestivi e frettolosi e questo non giova affatto al benessere organizzativo di una grande azienda.

Occorre che l'Agenzia delle Entrate ed il partner tecnologico **avochino a se, in quanto titolare e conduttore, tutte le responsabilità civili e penali** previste dal Provvedimento del Garante per cominciare a costruire con la **fattiva e collaudata collaborazione dei Gestori di Rete, opportunamente addestrati ed inquadrati**, un nuovo sistema adeguato alle necessità presenti e future.

Per una migliore comprensione si allegano il provvedimento del Garante e quello dell'Agenzia delle Entrate.