TONUCCI & PARTNERS

Tonucci & Partners

In alliance with Mayer Brown LLP

CONFINDUSTRIA VICENZA

"*L'attuazione in azienda del Provvedimento del Garante privacy sugli Amministratori di Sistema: adempimenti pratici e soluzioni operative*".

VICENZA, 10 NOVEMBRE 2009

Prof. Avv. Alessandro Del Ninno

Tonucci & Partners

adelninno@tonucci.it

VARIE TAPPE DEL PROVVEDIMENTO SUGLI ADS

A) Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 *(G.U. n. 300 del 24 dicembre 2008).*

B) Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 12 febbraio 2009 *(G.U. n. 45 del 24 febbraio 2009)*

C) Amministratori di sistema: avvio di una consultazione pubblica - 21 aprile 2009 *(G.U. n. 105 dell' 8 maggio 2009).*

D) Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009 *(G.U. n. 149 del 30 giugno 2009)*

E) FAQ Amministratore di Sistema

Termine ultimo di attuazione: 15 Dicembre 2009.

Valore prescrittivo del Provvedimento sugli ADS: obblighi e sanzioni

TUTTO CIÒ PREMESSO IL GARANTE:

ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive *l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici…..*

Art. 162 – comma 2-*ter* del Codice della privacy

2-ter. In caso di ***inosservanza dei provvedimenti di prescrizione di misure necessarie*** *o di divieto di cui, rispettivamente,* ***all'articolo 154, comma 1, lettere c)*** *e d), è altresì applicata in sede amministrativa, in ogni caso,* ***la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.***

Art. 164-*bis*. Casi di minore gravità e ipotesi aggravate

1. Se taluna delle violazioni di cui agli articoli 161, 162, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.

2. In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, a eccezione di quelle previste dagli articoli 162, comma 2, 162-bis e 164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da cinquantamila euro a trecentomila euro. Non è ammesso il pagamento in misura ridotta.

3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al doppio.

4. Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

Ipotesi sanzionatorie concrete per violazione del Provvedimento sugli ADS

Violazione di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta: da Euro 12.000 ad Euro 72.000.

Violazione reiterata commessa anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni: da Euro 50.000 ad Euro 300.000. Non è ammesso il pagamento in misura ridotta.

Violazione di maggiore gravità (per numero di interessati coinvolti e per gravità del pregiudizio): da Euro 60.000 ad Euro 360.000.

Aumento del quadruplo se sanzioni inefficaci in ragione delle condizioni economiche del contravventore: da Euro 120.000 ad Euro 720.000.

DEFINIZIONE DI “AMMINISTRATORE DI SISTEMA”

E’ uno specialista in informatica – egli stesso utente della rete e/o dei sistemi amministrati - dotato di particolari diritti d’accesso alle risorse e con specifiche mansioni di gestione, manutenzione e controllo. Può essere – anche se non necessariamente - il responsabile della gestione di singoli PC o di PC collegati in rete (network).

Fra i suoi compiti vi sono l'installazione e l’aggiornamento di hardware e software, l'aggiunta o la rimozione di utenti autorizzati, l'assegnazione di credenziali di autenticazione, la risoluzione di problemi tecnici dei sistemi e/o della rete, il controllo delle prestazioni del sistema, la progettazione e la implementazione di nuove applicazioni, la manutenzione periodica dei sistemi (es: antivirus, back up, etc).

A QUALI AMMINISTRATORI SI APPLICA IL PROVVEDIMENTO DEL GARANTE?

Il Provvedimento si applica a tutti i soggetti ai quali il Titolare del trattamento abbia attribuito:

"*funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, di amministratore di base di dati, di amministratore di rete e di apparati di sicurezza e di amministratore di sistemi software complessi, laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali".*

TIPOLOGIE DI AMMINISTRATORI DI SISTEMA

Dunque il Provvedimento si applica a tutti i soggetti cui il Titolare abbia attribuito ruolo e funzioni tecniche "*propriamente corrispondenti o assimilabili*" a:

Application Software Administrator
Amministratore di un particolare tipo di applicazione.

System Administrator
Amministratore di sistema.

Network Administrator
Specializzato in reti di calcolatori e relativi apparati di networking come router, bridge e switch. Traducibile con amministratore di rete.

Security Administrator
Specializzato nella gestione della sicurezza al confine del sistema.

Database Administrator
Specializzato nell'amministrazione di basi di dati.

COME INDIVIDUARE IN CONCRETO GLI AMMINISTRATORI DI SISTEMA ALL'INTERNO DELL'ORGANIZZAZIONE DEL TITOLARE DEL TRATTAMENTO?

In assenza di una precisa definizione normativa dell'amministratore di sistema (che invece esisteva nell'abrogato Regolamento 318/1999, anche se di portata inferiore rispetto alla figura disciplinata ora), vi sono anche altre indicazioni contenute nel Provvedimento che possono supportare il Titolari del trattamento nel comprendere come individuare all'interno della propria organizzazione gli amministratori di sistema.

Una prima indicazione (organizzativa) emerge dalla parte del Provvedimento in cui il Garante suggerisce che:

"*Gran parte dei compiti previsti nel Disciplinare Tecnico - Allegato B al Codice della privacy 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 e di autorizzazione*".

COME INDIVIDUARE IN CONCRETO GLI AMMINISTRATORI DI SISTEMA ALL'INTERNO DELL'ORGANIZZAZIONE DEL TITOLARE DEL TRATTAMENTO?

Per qualificare un "*amministratore di sistema*" in base a quanto previsto dal Provvedimento (e dunque per sottoporre tale figura agli obblighi ivi previsti) il Titolare del trattamento deve riferirsi anche **a particolari elementi soggettivi**.

Infatti, per il Garante, l'amministratore di sistema **non è qualificato solo dalle oggettive attività tecniche che svolge**, ma deve essere altresì un soggetto che nello svolgimento di dette attività:

A. agisce quale **professionista altamente qualificato** dal punto di vista tecnico;
B. ha **un'effettiva ed elevata capacità di azione tecnica propria** rispetto alle informazioni trattate;
C. riveste un ruolo tecnico particolarmente **rilevante, specifico e critico**;
D. è legato al titolare del trattamento da un rapporto **avente natura fiduciaria** (data l'autonomia delle sue azioni);
E. è una figura **solitamente centrale** nei piani di sicurezza e nei DPS delle aziende.

COME INDIVIDUARE IN CONCRETO GLI AMMINISTRATORI DI SISTEMA ALL'INTERNO DELL'ORGANIZZAZIONE DEL TITOLARE DEL TRATTAMENTO?

Inoltre, è lo stesso Garante privacy che chiarisce che:

Non rientrano nella definizione di "amministratore di sistema" tutti i soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

FINALITA' DEL PROVVEDIMENTO SUGLI ADS

Le finalità del Provvedimento possono sinteticamente e concretamente riassumersi come segue.

Le prescrizioni operative mirano ad evitare o per lo meno gestire i rischi connessi a trattamenti di particolari delicatezza (cfr. art. 17 Codice privacy):

A. derivanti dal fatto che gli amministratori di sistema, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative **che possono comportare elevate criticità rispetto alla protezione dei dati;**

B. connessi allo svolgimento, da parte dell'AdS, di attività tecniche che comportano, in molti casi, **un'effettiva capacità di azione autonoma** sulle informazioni trattate (necessità di bilanciamento dell'autonomia tecnica);

FINALITA' DEL PROVVEDIMENTO SUGLI ADS

C) derivanti dalla scarsa consapevolezza dei Titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici circa i **rischi e le criticità implicite nell'affidamento degli incarichi di amministratore di sistema**;

D) derivanti dall'assenza di idonee misure di carattere organizzativo nell'ambito di organizzazioni ed enti pubblici e privati, assenza che si traduce per i Titolari del trattamento **nella totale inconsapevolezza dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, della stessa identità dei soggetti che operano quali amministratori di sistema** in relazione ai diversi servizi e banche di dati.

LE IMPRESE SOGGETTE AL PROVVEDIMENTO SUGLI ADS

Il Provvedimento si applica a **tutti i titolari di trattamenti di dati personali - sia nel settore pubblico che nel settore privato** - soggetti all'ambito applicativo del Codice **ed effettuati con strumenti elettronici**, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice).

IMPRESE NON SOGGETTE ALL'OBBLIGO

Il Provvedimento **non si applica** ai trattamenti di dati personali effettuati in ambito pubblico e privato **a fini amministrativo-contabili che pongono minori rischi per gli interessati** e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008).

D.L. 112/2008 ART. 29

Art. 29.
Trattamento dei dati personali

1. All'articolo 34 del codice in materia di protezione dei dati personali,dopo il comma 1 e' aggiunto il seguente:

*« 1-bis. 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 ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, **nonche' a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani**, il Garante, sentito il Ministro per la semplificazione normativa, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di cui al comma 1»*

Quali sono in concreto le imprese escluse in quanto svolgono esclusivamente trattamenti per correnti finalità amministrative e contabili in qualità di piccole e medie imprese, liberi professionisti o artigiani?

La risposta è contenuta nel decreto ministeriale del 18 Aprile 2005 (d.m. Sviluppo Economico) recante i criteri di individuazione di “microimpresa”, “piccola impresa” e “media impresa”.

DEFINIZIONE DI MICROIMPRESA

Nell'ambito della categoria delle PMI, si definisce microimpresa l'impresa che:

a) ha meno di 10 occupati, e

b) ha un fatturato annuo oppure un totale di bilancio annuo non superiore a 2 milioni di euro.

[I due requisiti di cui alle lettere a) e b) sono cumulativi, nel senso che tutti e due devono sussistere].

DEFINIZIONE DI PICCOLA IMPRESA

Nell'ambito della categoria delle PMI, si definisce piccola impresa l'impresa che:

a) ha meno di 50 occupati, e

b) ha un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro.

[I due requisiti di cui alle lettere a) e b) sono cumulativi, nel senso che tutti e due devono sussistere].

DEFINIZIONE DI MEDIA IMPRESA

Nell'ambito della categoria delle PMI, si definisce media impresa l'impresa che:

a) ha meno di 250 occupati, e

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

[I due requisiti di cui alle lettere a) e b) sono cumulativi, nel senso che tutti e due devono sussistere].

DEDUZIONI SUL CAMPO DI ESCLUSIONE DEL PROVVEDIMENTO SUGLI ADS

Se ne deve dedurre logicamente che quando il Garante afferma che:

"gli accorgimenti e le misure vengono prescritti ai sensi dell'art. 154, comma 1, lett. c) del Codice a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione" (Punto 4 del Provvedimento sugli ADS);

" *i soggetti che possono avvalersi della semplificazione sono – tra gli altri – quelli che trattano dati personali* ***unicamente*** *per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese come definite dall'art. 2083 cod. civ. e dal d.m. 18 aprile 2005, recante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese*" (Punto 1, lettera b) del Provvedimento di semplificazione del 27 Novembre 2008).

DEDUZIONI SUL CAMPO DI ESCLUSIONE DEL PROVVEDIMENTO SUGLI ADS

La conseguenza è l'inapplicabilità del Provvedimento sugli amministratori di sistema a tutti i Titolari del trattamento rappresentati da micro, piccole o medie imprese così come definite dal d.m. del 18 Aprile 2005 e che trattano dati personali esclusivamente per finalità contabili o amministrative.

DEFINIZIONE DI FINALITA' CONTABILI E AMMINISTRATIVE

Pur non esistendo una precisa definizione normativa, può desumersi dagli stessi provvedimenti di semplificazione del Garante (es: Provv. 19 Giugno 2008) in materia che tali trattamenti hanno ad oggetto:

A. dati ovviamente diversi da quelli sensibili o giudiziari;

B. dati attinenti ad altre imprese, amministrazioni, clienti, fornitori e dipendenti utilizzati in relazione a obblighi contrattuali e normativi;

C. dati inerenti gestione di ordinativi, buste paga, ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in *outsourcing*, dipendenti;

D. trattamenti relativi all'ordinaria attività di supporto delle aziende, come ad esempio dati relativi alla gestione dell'autoparco, alle procedure di acquisto dei materiali di consumo, alla manutenzione degli immobili sociali, etc (cfr. FAQ 24).

ALTRI CASI DI ESCLUSIONE

Va altresì ricordato che dal momento che il Provvedimento sugli Amministratori di Sistema **è obbligatorio solo per i Titolari del trattamento** (che impiegano strumenti elettronici), **esso sarà inapplicabile ai trattamenti che – per conto del titolare – siano svolti da imprese terze nominate responsabili del trattamento.**

Per meglio comprendere:

1. Se il titolare affida ad un'azienda terza servizi di amministrazione di sistema in *outsourcing* (esempio di servizi di gestione sistemistica, i servizi di housing, hosting, gestione applicativa, archiviazione remota, etc) e nomina detta impresa "responsabile del trattamento", **ciò non consente anche una delega delle responsabilità connesse al provvedimento sugli Ads** (delle cui eventuali violazioni resterà comunque responsabile giuridicamente il titolare, anche se commesse dall'*outsourcee*).

2. Diventa **dunque fondamentale** per il titolare del trattamento curare con **grande attenzione il contratto di affidamento** oppure (se non c'è contratto) **l'atto di nomina a responsabile del trattamento** dell'impresa terza, per poter "recuperare" e far valere una corresponsabilità dell'outsourcee (per inadempimento del contratto o dell'atto di nomina) in caso di violazione del Provvedimento sugli Ads.

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

Valutazione delle caratteristiche soggettive come presupposto della nomina degli AdS.

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.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

Come si valutano le capacità dell'amministratore di sistema?

In che modo può essere correttamente svolta tale valutazione preliminare e, soprattutto, documentata in caso di ispezione del Garante?

È ovvio che si parte dal presupposto che chi di fatto svolge già oggi la funzione di amministratore di sistema sia in grado si svolgere la propria funzione; può essere allora organizzativamente opportuno predisporre una sorta di curriculum vitae di ciascun amministratore che indichi chiaramente titoli di studio, certificazioni professionali, esperienze professionali, corsi di formazione già svolti.

Il CV deve essere datato e firmato sia dall'amministratore che dal titolare.

L'indicazione dei percorsi formativi svolti specie per gli ambiti **non prettamente tecnologici ma relativi invece alle problematiche della privacy e della protezione dei dati personali assume un valore particolarmente importante** per il "*rispetto della garanzia delle vigenti disposizioni*". **L'amministratore di sistema non può essere solo un bravo tecnico ma deve conoscere la normativa sulla privacy.**

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

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.

Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema (almeno: nome, cognome, funzione o area organizzativa di appartenenza), con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Non vi è più l'obbligo di annotare gli estremi anche nel DPS (cfr. Provv. Gar. 25 Giugno 2009)

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

Informativa su AdS aventi accesso a dati personali dei lavoratori.

Qualora l'attività degli amministratori di sistema riguardi **anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori**, i titolari pubblici e privati nella qualità di datori di lavoro **sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni**, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti (possibile applicazione del nuovo art. 161 del Codice della privacy).

Modalità:

a) informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare;
b) disciplinare tecnico su email e Internet;
c) altri strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini).

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

Informativa su AdS aventi accesso a dati personali dei lavoratori: deroga.

La conoscibilità degli AdS aventi accesso ai dati personali dei lavoratori nell'ambito di un idoneo sistema di pubblicità interna **è un obbligo che può essere derogato** in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Tale deroga appare concretamente possibile in ambito pubblico.

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

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 o dei responsabili 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.

L'obbligo della verifica annuale non è nuovo, ma specifica solo rispetto al peculiare ruolo di AdS quanto già previsto per gli incaricati del trattamento dai **punti nn. 14 e 15 del Disciplinare Tecnico – Allegato B al Codice della privacy**.

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e ***addetti alla gestione o alla manutenzione degli strumenti elettronici****, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

Nota: contrasto tra obblighi di designazione nominativa degli AdS e punto n. 15 del Disciplinare Tecnico.

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

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 essere:

a) complete;
b) Inalterabili;
c) verificabili sotto il profili della loro integrità;
d) adeguate al raggiungimento dello scopo per cui sono richieste;
e) inclusive dei riferimenti temporali e della descrizione dell'evento che le ha generate;
f) soggette a conservazione per almeno sei mesi.

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Tale obbligo può essere eventualmente delegato al responsabile del trattamento mediante una specifica istruzione contenuta nell'atto di nomina oppure mediante specifiche clausole contrattuali (cfr. punto 3-*bis* del Provv.).

Tale obbligo (relativo al solo caso in cui l'oggetto dell'outsourcing sia rappresentato da "*servizi di amministrazione di sistema*" in quanto tali) implica la necessità di una particolare attenzione ai profili contrattuali ed alle relazioni contrattuali tra le imprese.

ADEMPIMENTI OPERATIVI PREVISTI DAL PROVVEDIMENTO

Problematiche operative dei servizi di AdS conferiti in outsourcing.

La sede contrattuale diventa in tale ottica rilevante poiché destinata ad evitare a monte problemi rilevanti nel rapporto tra *outsourcer* e *outsourcee* ad esempio connessi:

a) all'obbligo per il titolare di previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato (che essendo esterno può essere poco conosciuto dall'outsourcer);
b) all'obbligo per l'impresa outsourcer di verificare annualmente l'operato di amministratori di sistema che possono essere dipendenti dell'impresa outsourcee (es: la verifica dell'operato degli AdS esterni in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza può comportare la lesione delle informazioni "organizzative, tecniche e di sicurezza" dell'outsourcee);

c) al fatto che gli obblighi devono essere adempiuti "a distanza" dall'impresa outsourcer (es: gestione degli elenchi degli AdS dell'impresa outsourcee ed eventuali modifiche per variazione delle attività).

QUALIFICAZIONE SOGGETTIVA "PRIVACY" DELL'AMMINISTRATORE DI SISTEMA: RESPONSABILE O INCARICATO DEL TRATTAMENTO?

Il Provvedimento lascia liberi i titolari del trattamento di designare gli AdS nel quadro più generale delle nomine a responsabile o incaricato del trattamento, tuttavia – a livello organizzativo – le seguenti considerazioni appaiono rendere **più coerente la scelta di inquadrare gli AdS nell'ambito soggettivo di Responsabili del trattamento**:

a) lo stesso Garante prescrive che "*l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e 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*", **sostanzialmente prevedendo le identiche qualifiche soggettive obbligatorie menzionate dall'art. 29 del Codice della privacy per il Responsabile del trattamento**;

QUALIFICAZIONE SOGGETTIVA "PRIVACY" DELL'AMMINISTRATORE DI SISTEMA: RESPONSABILE O INCARICATO DEL TRATTAMENTO?

b) lo stesso Garante prescrive che "*anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29*";
c) la natura giuridica della figura dell'incaricato del trattamento ("*persona fisica che opera sotto la diretta autorità del titolare o del responsabile*") contrasta con l'ampia autonomia e facoltà di azione propria dell'operato degli amministratori di sistema;
d) la nomina a responsabile appare più coerente nell'ambito dei servizi di amministrazione di sistema affidati in outsourcing;
e) dal punto di vista organizzativo, il titolare del trattamento non potrebbe avvalersi delle facoltà semplificate di nomina degli incaricati di cui all'art. 30.2 del Codice della privacy (visti gli obblighi di designazione comunque individuale degli Ads).

LA RESPONSABILITA' DELL'AMMINISTRATORE DI SISTEMA

In linea generale, le potenziali responsabilità dell'Ads dipendono, in gran parte, dal tipo di ruolo (molto articolato e complesso o piuttosto ridotto) assegnato dal titolare di trattamento.

In relazione al crescere dell'ampiezza di ruolo affidato crescono gli spazi di autonomia e di libertà delle condotte e, conseguentemente, le possibili responsabilità giuridiche dell'amministratore. **Esse, peraltro, non escludono secondo le regole generali, una responsabilità "in eligendo" o "in vigilando" del titolare di trattamento.**

Tenendo ben distinti i due diversi piani della responsabilità in cui può incorrere l'azienda per violazione del provvedimento sugli Ads e della responsabilità personale dell'amministratore di sistema, per quest'ultimo possono individuarsi ipotesi di responsabilità assai diverse tra loro:

a) responsabilità per violazioni penalmente rilevanti;
b) responsabilità per inadempimento degli obblighi di cui al rapporto di lavoro;
c) responsabilità per violazione contrattuale;
d) responsabilità per violazione del Codice privacy o delle norme lavoristiche.

LA RESPONSABILITA' DELL'AMMINISTRATORE DI SISTEMA

Responsabilità penali.

In primo luogo, è lo stesso Garante nel Provvedimento ad evidenziare la rilevanza penale di certe condotte dell'Ads, potendo egli incorrere (secondo l'interpretazione del Garante), qualora abusi della qualità di operatore del sistema, in reati quali, ad esempio, **l'accesso abusivo a sistema informatico telematico** (art. 615-ter), la **frode informatica** (art. 640-ter), il **danneggiamento di informazioni, dati e programmi inf**ormatici (art. 635-bis e -ter) e il **danneggiamento di sistemi informatici telematici** (art. 635-quater e -quinquies).

Inoltre, l'Amministratore di sistema, ricorrendo i presupposti della norma, potrebbe commettere il reato di **trattamento illecito di dati personali** di cui all'art. 167 del Codice.

Da non escludere, inoltre, i potenziali "pericoli giuridici" derivanti dall'art. 169 (**omessa adozione delle misure di sicurezza**): pur essendo un reato tendenzialmente destinato al titolare di trattamento, non è da escludere che egli possa, mediante delega, trasferire importanti funzioni in materia all'Amministratore con conseguenze anche ai fini della responsabilità penale.

LA RESPONSABILITA' DELL'AMMINISTRATORE DI SISTEMA

Responsabilità penali dell'amministratore alla luce delle eventuali responsabilità dell'impresa ai sensi del d.lgs. 231/2001: cenni.

Oltre ai necessari interventi in materia di organizzazione, formazione e comunicazione da attuare, **si ricordano gli eventuali profili di responsabilità dell'impresa anche in relazione alla possibilità che, unitamente a violazioni in materia di dati personali, vengano commessi dall'Amministratore di sistema reati previsti dal D.Lgs. n. 231/2001 (frode informatica, accesso abusivo a sistema informatico, danneggiamento, ecc.).**

Per i suddetti reati se commessi da tali figure infatti, oltre alle responsabilità personali con relative aggravanti di pena, possono comunque essere attribuite responsabilità amministrative in capo alla Società in quanto le misure adottate non si sono rivelate adeguate.

LA RESPONSABILITA' DELL'AMMINISTRATORE DI SISTEMA

Responsabilità per inadempimento degli obblighi di cui al rapporto di lavoro.

Laddove l'amministratore di sistema sia un lavoratore dell'azienda, la eventuale violazione degli obblighi e delle istruzioni analitiche ricevute dal datore di lavoro/titolare del trattamento può comportare le responsabilità "lavoristiche" di cui agli articoli 2104 e 2105 c.c. con conseguente applicazione delle sanzioni disciplinari proprie di cui all'art. 2106 c.c.

LA RESPONSABILITA' DELL'AMMINISTRATORE DI SISTEMA

Responsabilità per violazione contrattuale.

Nel caso in cui le attività dell'amministratore di sistema siano esternalizzate (es: outsourcing), la violazione degli obblighi e delle istruzioni impartite può comportare una responsabilità contrattuale per inadempimento (es: contratto consulenziale per servizi di amministrazione di sistema stipulato con esperti).

Non è escluso che tale responsabilità contrattuali possa attivarsi anche contro l'azienda (outsourcee) cui è addetto l'amministratore di sistema esterno, con ulteriori profili di responsabilità specificatamente attinenti al rapporto tra azienda outsourcee e "suo" amministratore di sistema.

LA RESPONSABILITA' DELL'AMMINISTRATORE DI SISTEMA

Responsabilità per violazione del Codice privacy o delle norme lavoristiche.

Ulteriori ipotesi di responsabilità dell'amministratore di sistema (soprattutto laddove le relative attività siano ad esso delegate tecnicamente dal titolare del trattamento) possono sinteticamente illustrarsi come segue:

a) responsabilità amministrativa o penale per violazione dell'art. 162-bis del Codice della privacy (inosservanza degli obblighi di *data retention* di cui al d.lgs. 109/2008);
b) responsabilità penale per violazione del divieto di controllo a distanza dei lavoratori (art. 4 L. 300/1970 e artt. 113, 114 e 171 del Codice della privacy);
c) Responsabilità risarcitoria per "danno da trattamento dei dati personali" ex art. 15 del Codice della privacy ("***Chiunque*** *cagiona danni ad altri per effetto …..").*

DOMANDE E RISPOSTE PRATICHE SUGLI AMMINISTRATORI DI SISTEMA

Nel momento in cui il provvedimento del Garante attribuisce responsabilità all'Amministratore di sistema legandole anche ad un implicito riconoscimento di capacità e di affidabilità, può accadere che si crei uno nuovo status aziendale che inneschi rivendicazioni?

Non c'è questo rischio. Gli Amministratori di Sistema sono solo particolari Responsabili o Incaricati del trattamento, e dalla nomina non discende alcuna implicazione "lavoristica", come non ve ne sono quando si nominano in generale altri responsabili o incaricati.

E’ possibile eventualmente differenziare livelli di responsabilità per gli Amministratori di sistema?

Certamente, anzi il presupposto del Provvedimento è proprio quello di individuare le specifiche e diverse funzioni (e connesse responsabilità) dei vari ADS. Più in particolare, il Provvedimento prevede che prevede che all'atto della designazione di un amministratore di sistema, venga fatta "elencazione analitica" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato (che può essere diverso da amministratore ad amministratore), ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti.

DOMANDE E RISPOSTE PRATICHE SUGLI AMMINISTRATORI DI SISTEMA

A cosa va incontro un dirigente o un responsabile di unità organizzativa, che per motivi di urgenza, chiede ad un dipendente non abilitato in precedenza di svolgere alcune attività per le quali di norma è richiesto l'intervento di un Amministratore di sistema?

In teoria il dipendente non autorizzato sarebbe posto nella condizione di accedere a dati personali in violazione dell'ambito del trattamento consentito, quindi il dirigente autorizzerebbe un "accesso abusivo" ai dati e una violazione del profilo di autorizzazione concesso al dipendente. Se poi tale dipendente accedesse anche ai dati di lavoratori, vi sarebbe la violazione del Provvedimento nella parte in cui obbliga ad informare i lavoratori e ad elencare nominativamente nello specifico gli ADS che trattano dati dei lavoratori (visto che questo dipendente non sarebbe neanche un ADS, potrebbe essere contestata la violazione del Provvedimento sul punto).

DOMANDE E RISPOSTE PRATICHE SUGLI AMMINISTRATORI DI SISTEMA

In un caso specifico, l'Amministratore di sistema, come specificato nella lettera, è direttamente e personalmente responsabile dell'aggiornamento dei prodotti sistemistici. Può capitare frequentemente che l'Amministratore stesso, a fronte della necessità di un aggiornamento (richiesto ufficialmente dal produttore/fornitore, il quale segnala anche le criticità derivanti dal mancato aggiornamento) non possa procedere, in quanto ciò non gli è consentito, prevalentemente, per problemi di continuità del servizio (poiché occorre assicurare l'operatività ventiquattro ore su ventiquattro, non è possibile procedere, anche per diversi mesi, alla interruzione dei sistemi per effettuare gli aggiornamenti).
In questo caso come è cautelato l'amministratore di sistema? Occorre inserire una clausola ad hoc nella lettera di designazione?

All’atto della designazione individuale, il titolare o il responsabile dovranno impartire istruzioni che possano essere oggettivamente eseguite dall’amministratore. Se vi sono compiti che l’amministratore non può concretamente porre in essere, non vi potrà essere una responsabilità personale per violazione di istruzioni ineseguibili.

In virtù di quanto sopra, non è necessario, ma può valutarsi in un’ottica di mera opportunità l’inserzione di una clausola generale nella lettera di designazione del tipo di quella che segue:

Lei dovrà altresì segnalare allo scrivente, titolare del trattamento, o al soggetto da questi delegato qualsiasi situazione che, anche potenzialmente, non la metta in grado oggettivamente e/o a causa di politiche aziendali in essere di dare corretta e tempestiva esecuzione alle istruzioni fornite, conformandosi successivamente alle indicazioni e/o alle istruzioni addizionali che il titolare o il soggetto da questi delegato avranno cura di fornirle prontamente.

GRAZIE PER L'ATTENZIONE