



## IMPORTANTI NOVITA' INTRODOTTE CON UN RECENTE PROVVEDIMENTO DEL GARANTE DELLA PRIVACY

### PRIVACY

CON IL PRESENTE DOCUMENTO BLB STUDIO LEGALE INTENDE FORNIRE UN RAPIDO AGGIORNAMENTO RELATIVO AL QUADRO NORMATIVO E REGOLAMENTARE IN MATERIA DI PRIVACY (D.LGS. 196/2003) - "CODICE DELLA PRIVACY" CHE INTRODUCE ALCUNE IMPORTANTI NOVITÀ IN RELAZIONE AGLI ADEMPIMENTI IMPOSTI AI "TITOLARI DEL TRATTAMENTO"

**1. Nomina dell'amministratore di sistema e adempimenti organizzativi.**

**2. Aumento delle sanzioni amministrative per violazione del Codice della privacy.**

#### **1. Nomina dell'amministratore di sistema e adempimenti organizzativi.**

Con il provvedimento del 27 Novembre 2008, pubblicato nella G.U. del 24 Dicembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", il Garante ha introdotto le seguenti misure ai titolari dei trattamenti di dati personali che rientrano nel campo di applicazione del Codice e che sono effettuati con strumenti elettronici. La riforma non riguarda i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili.

##### *A. Valutazione delle caratteristiche soggettive.*

Il conferimento dell'incarico di "amministratore di sistema" deve essere effettuato previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto da nominare, il quale è tenuto a fornire idonea garanzia del pieno rispetto della vigente normativa in materia di trattamento, compreso il profilo relativo alla sicurezza.

##### *B. Designazioni individuali.*

Il conferimento dell'incarico di "amministratore di sistema" deve essere individuale e contemplare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

##### *C. Elenco degli amministratori di sistema.*

Gli estremi dei soggetti (persone fisiche) nominati amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Documento Programmatico sulla sicurezza oppure, qualora il titolare non sia tenuto a redigerlo, annotati in un documento interno che deve essere sempre tenuto aggiornato e disponibile in caso di accertamenti da parte del Garante. Se l'attività degli amministratori di sistema riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari del trattamento 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 informativi cui questi sono preposti, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico previsto dal provvedimento del Garante n. 13 del 1° marzo 2007 (Linee Guida su e-mail e Internet nel rapporto di lavoro) o, in alternativa, mediante altri strumenti di comunicazione interna (ordini di servizio, bollettini interni, intranet aziendale). Sono fatti salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con previsioni legislative che



disciplinino uno specifico settore.

#### *D. Servizi in outsourcing*

Qualora il servizio di amministrazione di sistema venga affidato in outsourcing, il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche nominate amministratori di sistema.

#### *E. Verifica delle attività.*

L'operato degli amministratori di sistema deve essere verificato, con cadenza almeno annuale, da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalla vigente normativa.

#### *F. Registrazione degli accessi.*

Devono essere adottati tutti i 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 adeguate allo scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo non inferiore a sei mesi.

## **2. Aumento delle sanzioni amministrative per violazione del Codice della privacy.**

Il decreto-legge del 30 Dicembre 2008, n. 207 ha introdotto rilevanti modifiche all'impianto sanzionatorio del Codice della privacy. Le sanzioni amministrative in caso di violazione delle regole sul trattamento dei dati personali sono state considerevolmente aumentate. Il decreto-legge è già in vigore dal 30.12.2008.

Queste le novità introdotte dal decreto.

#### *A. Omessa o inidonea informativa sul trattamento dei dati personali (art. 161 Codice privacy)*

L'omessa o inidonea informativa (precedentemente punita con la sanzione da 3 a 18 mila euro per trattamenti di dati comuni) è ora sanzionata con una pena pecuniaria da 6 a 36 mila Euro. In tutti i casi è possibile l'aumento della sanzione fino al triplo (dunque il massimo della sanzione previsto dal decreto potrebbe essere in questi casi di 108 mila euro).

#### *B. Violazione degli obblighi in materia di misure minime di sicurezza (art. 162 Codice privacy). Inosservanza dei provvedimenti del Garante.*

Sono stati inseriti due nuovi comma, 2-bis e 2-ter, dell'art. 162: il primo prevede che in caso di trattamento di dati personali effettuato in violazione delle misure minime indicate nell'articolo 33 del Codice o delle disposizioni indicate nell'articolo 167 del Codice, è applicata in sede amministrativa la sanzione del pagamento di una somma da ventimila euro a centoventimila euro. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta. Il comma 2-ter sanziona l'inosservanza di prescrizioni del Garante con il pagamento di una somma da trentamila euro a centottantamila euro.

#### *C. Omessa o incompleta notificazione dei trattamenti al Garante (art. 163 Codice privacy).*

La omessa o incompleta notifica nei casi in cui è dovuta è ora punita con la sanzione da 20 mila le ipotesi di violazioni amministrative menzionate nel nuovo Capo.

#### *D. Omessa adozione di misure di sicurezza (art. 169 Codice privacy).*

Ai sensi dell'art. 169, la sanzione per l'omessa adozione delle misure di sicurezza è l'arresto fino a due anni; è stato cancellato il riferimento all'ammenda; il meccanismo di oblazione è stato modificato nel senso che il pagamento che estingue il reato di omessa adozione delle misure di sicurezza è stato portato a 30 mila euro (prima erano 12.500 Euro). Il pagamento in oblazione è diverso dalla sanzione amministrativa che va applicata "in ogni caso" e senza che sia possibile "il pagamento in misura ridotta" di cui all'art. 162, comma 2-bis. Quindi un'azienda potrebbe dover pagare 30 mila euro per estinguere il reato e inoltre una somma tra 20 mila e 120 mila euro per non aver adottato le misure minime poi implementate.

#### *E. Nuovo articolo 164-bis del Codice della privacy.*

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.

**B | L | B**

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.

*F. Violazione dell'ordine del Garante di fornire informazioni e/o di esibire documenti (art. 164 Codice privacy).*

E' punita con la sanzione amministrativa da 10 a 60 mila Euro (prima era da 4 a 24 mila Euro).

*G. Cessione dei dati in violazione della disciplina rilevante.*

E' punita con la sanzione da 10 a 60 mila euro (prima da 5 a 30 mila euro);

*H. Comunicazione di dati sanitari non attraverso personale medico (art. 84 Codice privacy).*

E' punita con la sanzione amministrativa da mille a seimila euro (prima da 500 Euro a 3 mila euro);

*I. Violazione dell'art. 162-bis in materia di data retention (applicabile solo a fornitori di servizi di comunicazione elettronica).*

E' stato eliminato l'aumento fino al triplo della sanzione che era stata già introdotta dal d. lgs. 109/2008 (da 10 a 50 mila euro).

Per eventuali approfondimenti: **BLB Studio Legale**

+39.02.80.52.650

+39.06.35.40.16.37