Vigilanza più "vigilata" negli aeroporti

14 Dicembre 2009 - Vigilanza più "vigilata" negli aeroporti Vigilanza più "vigilata" negli aeroporti - Accessi alle aree riservate con impronte digitali - Il Garante per la protezione dei dati personali ha autorizzato una società, che svolge attività di vigilanza e sicurezza aeroportuale, a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti Newsletter Gararnte privacy -n. 332c del 10 dicembre 2009

Vigilanza più "vigilata" negli aeroporti - Accessi alle aree riservate con impronte digitali - Il Garante per la protezione dei dati personali ha autorizzato una società, che svolge attività di vigilanza e sicurezza aeroportuale, a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti **Newsletter Gararnte privacy -n. 332 del 10 dicembre 2009**

Newsletter Gararnte privacy -n. 332 del 10 dicembre 2009

Vigilanza più "vigilata" negli aeroporti

Accessi alle aree riservate con impronte digitali

Il Garante per la protezione dei dati personali ha autorizzato una società, che svolge attività di vigilanza e sicurezza aeroportuale, a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti di Milano "Linate" e "Malpensa", Roma "Fiumicino", Venezia e Pisa. L'azienda aveva sottoposto alla verifica preliminare del Garante un progetto che prevedeva la possibilità di rilevare con il sistema biometrico la presenza dei lavoratori. Il progetto escludeva comunque il controllo sull'orario di lavoro.

L'esigenza della società era quella di scongiurare accessi indebiti nelle cosiddette "aree sterili" (security restricted area) degli aeroporti, ovvero nelle zone preposte ai controlli pre-volo dei passeggeri, dei bagagli a mano e da stiva, delle merci e degli operatori aeroportuali di staff. Per tali aree il "Programma Nazionale di Sicurezza" prevede non solo limitazioni di accesso, ma anche particolari misure di sicurezza necessarie per prevenire, ad esempio, l'introduzione a bordo degli aeromobili di armi, ordigni esplosivi e qualsiasi altro oggetto pericoloso.

Il sistema biometrico contenuto nel progetto si basa sul confronto tra le impronte digitali rilevate e il template (la rappresentazione in codice numerico), memorizzato e cifrato su una smart card nell'esclusiva disponibilità del lavoratore, che ha prestato preventivamente il proprio specifico consenso al trattamento dei dati.

L'Autorità (con un provvedimento di cui è stato relatore Mauro Paissan) ha ritenuto proporzionati la raccolta e l'uso delle impronte digitali dei dipendenti in relazione agli accessi alle sole "aree sterili". Ha tuttavia prescritto alla società di prevedere modalità alternative di accesso e identificazione e di fornire ai dipendenti un'apposita informativa che indichi la natura facoltativa del consenso al trattamento dei dati biometrici. I dati relativi agli accessi alle "aree sterili" potranno essere conservati per un tempo massimo di sette giorni.