Temi: Biometria
Categoria professionale: Dirigente
Tipologia di dati: Biometrici

Posso raccogliere le impronte biometriche dei miei collaboratori?

La direzione desidera evitare ai suoi collaboratori di dover sempre portare una chiave magnetica per entrare nell'edificio e timbrare. Decide di mettere all'opera un controllo biometrico degli accessi. I collaboratori sono convocati tramite corrispondenza interna per fornire le loro impronte biometriche (geometria della mano e impronte digitali).
Tre impiegati mancano all'appello. Invitati a spiegarsi, dichiarano di essersi informati che l'uso di un tale dispositivo costituirebbe una grave lesione della loro personalità e rifiutano di sottomettersi alla raccolta delle impronte.
La direzione s'informa meglio sulle misure da rispettare quando s'installa e utilizza un tale sistema. Contatta il consigliere alla protezione dei dati dell'impresa o l'incaricato federale/cantonale. Convoca poi l'insieme dei collaboratori per discutere dei vantaggi del nuovo sistema. Li informa d'aver preso contatto con le autorità competenti e di poter garantire che il sistema non sarà utilizzato in modo abusivo, che i dati saranno conservati in modo sicuro, ecc. Uno degli impiegati non demorde: esistono dei mezzi più semplici per controllare l'accesso ai locali, come ad esempio le carte magnetiche. La direzione propone allora un voto a mano alzata. I tre impiegati recalcitranti chiedono che il voto si svolga a urne segrete, cosa che ottengono.
Lo spoglio del voto viene eseguito: vince lo statu quo. La direzione ammette che la raccolta dei dati progettata non è proporzionata allo scopo prefisso e che è dunque necessario ottenere il consenso di ciascun impiegato. Visto i costi e le complicazioni che genererebbero la presenza di due sistemi paralleli (magnetici e biometrici), aggiorna il suo progetto e promette di studiare una soluzione meno invasiva.
I dati raccolti per permettere un controllo biometrico possono essere impiegati a dei fini estranei allo scopo annunciato. La direzione si congratula di aver favorito la ricerca di una soluzione creativa e rispettosa della integrità personale degli impiegati.

Raccomandazioni
I dati biometrici comprendono generalmente dei dati sensibili (in particolare sulla salute). Quand'è così, una base legale formale è necessaria e le persone interessate devono essere chiaramente informate e dare il loro consenso al trattamento di questi dati. Lo scopo perseguito deve essere chiaro e deve essere scelta la misura la più adeguata e meno invasiva per raggiungerlo. Questa misura deve fare oggetto di una comunicazione appropriata. Il datore di lavoro deve inoltre consultare gli impiegati o i loro rappresentanti e, in assenza di una base legale formale, ottenere il loro consenso libero e informato prima d'introdurre dei sistemi automatizzati per il trattamento dei dati personali.

Prinicipi di base
LIPAD 38 et 42 ; LPD 4 al. 4, 12 e 13 ; LL 6 ; OLL3 26 ; CO 328 e 328b

Protezione della personalità, protezione dei lavoratori, principi di liceità (legalità), buona fede e della proporzionalità: la misura deve essere adeguata, necessaria e il meno invasiva possibile.

Esempio concreto
La banca privata Pictet & Cie di Ginevra usa il riconoscimento facciale in 3D come misura di sicurezza d'accesso ai suoi edifici dal 2006. Com'è riuscita a sormontare i timori dei suoi 2000 collaboratori ?

Grazie alla comunicazione. Questa tecnologia non permette di monitorare lo stato di salute di un individuo e di violare la sua sfera privata. « I dipendenti temono a volte che la scannerizzazione del loro viso sia pericoloso per la salute, ma non è assolutamente così poiché l'apparecchio si limita a filmarli », nota Jean-Pierre Therre, responsabile della sicurezza della banca privata. La banca dati non contiene foto degli impiegati, ma unicamente l'analisi delle scannerizzazioni del loro cranio secondo 40.000 punti di riferimento: http://www.1234economy.com/biometrie-et-reconnaissance-faciale-en-3d-comment-la-banque-privee-genevoise-pictet-a-gere-les-resistances /