Soluzioni per la rilevazione delle presenze
del personale ed elaborazione dei cartellini

iClock.it

# Informazioni tecniche riguardo la tutela della privacy sul dispositivo con identificazione biometrica facciale e palmare

Riassumiamo qui di seguito i punti salienti riguardo le informazioni tecniche dei dispositivi biometrici in relazione alla protezione della privacy degli utenti.

Innanzitutto essi sono protetti con password di accesso e i campioni biometrici sono memorizzati solo sui dispositivi stessi con dati crittografati.

Le immagini non vengono mai memorizzate. Le caratteristiche di identificazione (punti di riferimento biometrici) sono generate dall'immagine attraverso un sofisticato algoritmo che li converte in un modello biometrico i cui punti caratteristici sono altamente concentrati e non vi è alcuna relazione di spazio e distanza tra di loro, e li memorizza sotto forma di un codice digitale.

Inoltre, l'algoritmo con cui sono generati questi codici digitali, sono tali per cui non permettono di ritornare indietro, quindi non consentono di ricostruire l'immagine del volto o del palmo della mano, ne il campione biometrico grezzo dei punti di riferimento da cui hanno avuto origine.

E' possibile abbinare il campione biometrico digitale solo ad numero progressivo (ID Utente) e non al cognome e nome dell'utente, rendendo così anonimo il codice digitale del modello biometrico associato alle transazioni di entrata ed uscita ad esso associate, come accade con il classico orologio lettore di tessere badge.

Questo numero utente sarà abbinato ad un nominativo sul software di gestione delle presenze installato sul Computer Server dell'ufficio personale, in cui **non** è memorizzato alcun campione biometrico, e che è soggetto alle usuali misure di sicurezza informatica, quali copie di salvataggio, password di accesso, protocolli di sicurezza di rete informatica e sistemistica, naturalmente a cura del servizio tecnico informatico che segue l'infrastruttura informatica dell'azienda utilizzatrice.

L'azienda utilizzatrice, infine, deve adottare tutte le procedure atte minimizzare rischi, quali cancellazione dal dispositivo dei campioni biometrici degli utenti che non prestano più servizio, effettuare salvataggi su supporti di memorizzazione sicuri ed inaccessibili, ecc..

Quando i modelli e i modelli biometrici vengono rimossi dal dispositivo di timbratura esso garantisce la cancellazione completa cancellando il modello corrispondente e delle relative transazioni di entrata-uscita ad esso associate nel database e nella memoria del dispositivo.

Per approfondire informazioni riguardo la privacy invitiamo a leggere il documento del produttore dei dispositivi: “In che modo le tecnologie di verifica biometrica ZKTeco sono conformi al GDPR?”

https://zkteco.eu/news-center/news/how-is-zkteco-biometrics-gdpr-compliant

Bloomtech di Gava Enrico e Scalet Carlo snc - P.IVA e C.F. 03676400264
Via XXIV Maggio, 120 - 31015 Conegliano (TV) Tel 0438.451533 - Fax 0438.699960
Email: info@bloomtech.it - Pec: info@pec.bloomtech.it - Web: www.bloomtech.it