Regione Calabria
A.S.P. di Vibo Valentia
Prot. N° 22681
del 21.06.2019

# 1 VALUTAZIONE DI IMPATTO

## sull'utilizzo di sistemi di lettura di dati biometrici mediante identificazione dell'impronta digitale per la rilevazione della presenza in servizio.

L'Azienda Sanitaria Provinciale di Vibo Valentia si è determinata per l'installazione di sistemi di lettura di dati biometrici mediante identificazione dell'impronta digitale per la rilevazione della presenza in servizio.

A tal proposito si fa presente che l'Azienda negli ultimi anni è stata sottoposta a diverse attività investigative da parte delle preposte Autorità Giudiziarie, mettendo in evidenza fenomeni di assenteismo ed utilizzo fraudento del cartellino marcatempo.

L'Azienda è già dotata di un sistema automatizzato di rilevazione delle presenze: si tratta di un orologio marcatempo, che, attraverso un cartellino magnetico personalizzato (badge), rileva la presenza in servizio dei dipendenti.

Ha, altresì, un regolamento interno che disciplina l'orario di lavoro e un regolamento disciplinare che prevede sanzioni di diversa entità in relazione alla gravità del comportamento posto in essere.

Le misure adottate, tuttavia, non hanno consentito di evitare comportamenti illeciti e false attestazioni di presenza in servizio da una parte, seppur minoritaria, del personale.

L'Azienda ha deciso, pertanto, di installare un sistema di rilevazione biometrico al fine di porre un freno ai comportamenti illeciti e garantire la presenza in servizio e il rispetto dell'orario di lavoro da parte di tutti i dipendenti .

L'installazione e il funzionamento di un sistema di rilevazione biometrico comporta necessariamente il trattamento di dati biometrici.

I dati biometrici sono "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici" (art. 4 GDPR). Si tratta in sostanza di dati che, "direttamente, univocamente e in modo tendenzialmente stabile nel tempo, sono collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona".

Per la loro natura, quindi, rientrano nella categoria dei dati sensibili, ossia di quei dati che meritano una specifica protezione dal momento che il loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali delle persone fisiche, con gravissime ripercussioni sulla sfera personale degli interessati, in caso di impropria utlizzazione.

Il rischio, intenzionale o accidentale, consiste nella vulnerabilità di un asset o di un gruppo di asset tecnologici in grado di causare un trattamento illecito dei dati e il pericolo di furti di indentità .

La gravità del rischio risiede nella circostanza che i dati biometrici non sono modificabili e sono inscindibilmente legati all'individuo e costituiscono, quindi, una sorta di credenziale di autenticazione non revocabile e non sostituibile, la cui appropriazione da parte di soggetti non legittimati può prestarsi ad azioni fraudolente e compromettere l'efficacia di sistemi di sicurezza basati sul riconoscimento biometrico.

Le caratteristiche biometriche che lasciano traccia, come le impronte digitali, possono comportare il rischio di un' acquisizione indebita e prestarsi, teoricamente, a frodi e furti di identità.

Al fine di evitare di incorrere in tali rischi, è necessario verificare che il sistema biomentrico da implementare sia conforme alla normativa dettata dal GDPR e adotti una serie di misure di sicurezza volte a garantire la protezione dei dati personali trattati.

L'art. 9, comma 1, del GDPR dispone un divieto generale di trattamento dei dati sensibili, prevedendo, poi, al comma 2, delle deroghe specifiche.

Il trattamento dei dati biometrici per la rilevazione delle presenze e dell'orario di lavoro è riconducibile alla deroga di cui all'art. 9, comma 2 lett. b), del GDPR, secondo cui il trattamento dei dati sensibili è possibile qualora sia *"necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia del diritto del lavoro e della sicurezza sociale e protezione sociale....."* .

La normativa vigente prevede a carico dei soggetti pubblici in qualità di datori di lavoro specifici obblighi di controllo e conseguenti responsabilità in capo al personale dirigenziale e/o direttivo in genere, sul quale incombe la verifica quotidiana della presenza in servizio del personale assegnato.

L'uso di tecnologie biometriche ha, pertanto, una finalità legittima, ciò nonostante, deve essere effettuato nel pieno rispetto dei principi di liceità, necessità, proporzionalità e minimizzazione dei dati.

Il trattamento, come già ampiamente esposto, è lecito in quanto necessario per adempiere ad un obbligo del titolare del trattamento nonché per eseguire un compito di interesse pubblico o comunque connesso all'esercizio dei pubblici poteri di cui è investito.

E' necessario, in quanto i sistemi di rilevazione delle presenze, già in uso, si sono rivelati inefficaci così come le sanzioni disciplinari previste dal regolamento vigente per le ipotesi di inosservanza dell'orario di lavoro o falsa attestazione della presenza in servizio.

La finalità che si vuole perseguire con l'installazione del sistema biometrico è dunque quella di prevenire fenomeni di assenteismo e comportamenti fraudolenti di dipendenti infedeli che timbrano il cartellino per i colleghi, in realtà assenti dal lavoro.

Il trattamento biometrico dei dati appare, pertanto, proporzionato rispetto al fine che l'azienda si è proposta di perseguire.

Dalla scheda tecnica trasmessa dalla Ditta fornitrice del terminale biometrico, risulta, infine, rispettato il principio della minimizzazione dei dati.

Il sistema, infatti, non memorizza in alcun modo il dato biometrico, residente sul badge e letto solo al momento della timbratura. Il dipendente deve apporre sia il badge sia il dito sul marcatempo che confronta le informazioni lette e, se corrispondenti, trasmette al sistema centrale le sole informazioni di timbratura, ossia la matricola, la data, l'orario e la causale.

E' stata data assicurazione che il dato biometrico è volatile, ossia non è memorizzato in alcun database, né sotto forma di codifica numerica né sotto forma di immagine. Non viene trasmesso in rete, ma risiede in forma numerica crittografata sul badge in possesso e ad uso esclusivo del dipendente.

Il sistema è in grado di rilevare il cd. "dito vivo", nel senso che evita i comportamenti fraudolenti (ad esempio la copia dell'impronta in silicone), ma non prevede l'associazione dei dati biometrici con ulteriori informazioni riferite al dipendente.

La registrazione (cd. enrollment) viene effettuata avvalendosi di un personal computer e di un sensore ottico ad esso collegato attraverso un'interfaccia USB. L'immagine dell'impronta non viene memorizzata, se non per il tempo strettamente necessario alla sua elaborazione, né inviata al personal computelr, ma gestita completamente all'interno del dispositivo stesso.

L'impronta digitale, rilevata in sede di registrazione, è immediatamente trasformata, attraverso algoritmi unidirezionali biometrici in grado di convertire un'immagine in un blocco dati criptato, in una stringa di bits crittografati (template) ed inviata al personal computer che provvede a registrarla sotto forma di template sul supporto personale di identificazione, ossia una tessera "smart card" (carta MIFARE) dotata di micro chip cui è preventivamente associato un codice di identificazione personale c.d. "matricola". Subito dopo la creazione del blocco dati criptato, l'immagine viene rimossa.

Il processo è irreversibile: non è possibile convertire il blocco criptato in immagine .

Quando il terminale è configurato in modalità MIFARE, durante la registrazione delle immagini, il blocco dati criptato viene scritto direttamente sulla smart card, senza lasciare traccia dello stesso sul terminale e rendendo, in tal modo, impossibile la diffusione del dato biometrico nel database locale del terminale e via rete.

Non è altresì possibile ricavare l'immagine dell'impronta digitale partendo dal template memorizzato sulla smart card , in uso e custodia al dipendente.

Per quanto concerne il rilevamento della presenza, il terminale, in fase di riconoscimento del dipendente, ha due input: il dito del dipendente e la smart card datagli in uso.

L'utilizzatore fa leggere la carta Mifare al lettore e contemporaneamente pone il dito sul sensore biometrico, il quale elabora l'immagine dell'impronta al fine di ottenere il template e lo confronta con quello presente sulla card.

Se il confronto/riconoscimento ha esito positivo, il numero di matricola viene trasmesso al sistema di rilevazione che registra la matricola, la data, l'orario e la causale.

Anche in questa fase non c'è né la memorizzazione né la trasmissione di immagini dell'impronta e/o del template.

Le informazioni date dal fornitore sul funzionamento del sistema biometrico da installare garantiscono la volatilità del dato acquisito che non viene memorizzato in alcun database ma risiede soltanto, in forma criptata, sul badge in uso esclusivo del dipendente e viene letto solo al momento della timbratura.

Tenuto conto della finalità che l'Azienda intende perseguire e della modalità di funzionamento del sistema biometrico di registrazione e identificazione dell'impronta digitale per la rilevazione della presenza in servizio, si ritiene che il trattamento dei dati biometrici dei dipendenti possa essere effettuato in quanto lecito e rispettoso dei principi di necessità, proporzionalità e minimizzazione dei dati.

Nel rispetto dei principi di correttezza e trasparenza, l'Azienda, prima dell'inizio dei descritti trattamenti, deve, sulla base della normativa vigente, informare tutti i dipendenti del trattamento che si intende effettuare, delle sue finalità, delle modalità e delle misure di sicurezza adottate.

Deve altresì garantire agli interessati l'esercizio dei diritti di cui al Capo III del GDPR.

Per quanto sopra esposto, il Responsabile della Protezione Dati, Dott.ssa Maria Grazia Vavalà, dichiara che per le modalità di funzionamento del sistema di rilevazione dei dati biometrici e per le misure di sicurezza insite nel sistema medesimo, il trattamento dei dati biometrici dei dipendenti non presenta alcun rischio e si può, pertanto, procedere all'implementazione del sistema stesso, senza consultare preventivamente l'Autorità di Controllo (art. 36 del GDPR).

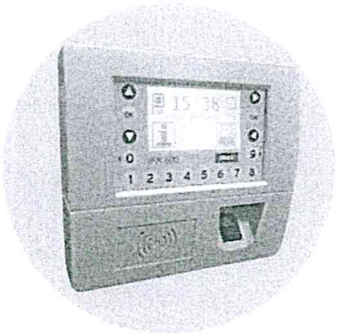
Il Responsabile della Protezione Dati

Dott.ssa Maria Grazia Vavalà

Il Direttore Generale Reggente

Dott.ssa Elisabetta Tripodi

# IFK 600 Biometrico



## Il terminale con tecnologia biometrica che garantisce sicuro riconoscimento

Ideale per Aziende, Enti Pubblici e Studi Professionali.

### PUNTI DI FORZA

- Elevate prestazioni e funzionamento in modalità on-line/off-line
- Dimensioni ridotte, qualità nel design (mm 165 x 158 x 60)
- Potenza, efficienza, affidabilità
- Semplicità nella manutenzione e aggiornamento
- Integrità dei dati grazie al sistema di criptatura

### FUNZIONI PRINCIPALI

- Rilevazione presenze
- Prenotazione / Fruizione pasti

### CARATTERISTICHE TECNICHE

- Display LCD 128x64 punti retro illuminato grafico
- Tastiera a membrana con 16 tasti
- Segnalatore acustico: Buzzer monotono
- Tecnologia di lettura: Lettore biometrico integrato + singola testina Mifare 13,56 MHz per comparazione impronta digitale
- Microprocessore a 32 bit con sistema operativo linux
- 128 MBytes di memoria DDR2
- 512 MBytes di memoria FLASH
- 800 Mhz CortexA8 CPU
- Orologio-datario ad alta precisione compensato in temperatura
- Porta Ethernet 10-100 Auto-MDIX, TCP/IP
- Una porta USB 2.0 per collegamento stampanti di scontrino e/o barcode reader
- Due relè (1A @50VAC) per apertura porta, suonerie etc.
- Facile ed immediata gestione dati, con la possibilità, a richiesta, di utilizzare unità di memoria rimovibile (ad esempio chiave USB) per una gestione dei dati off-line

### ALIMENTAZIONE, MANUTENZIONE E AGGIORNAMENTO

- Alimentazione 15 VDC (alimentatore esterno fornito a corredo)
- RICEVITORE POE integrato per alimentazione diretta da switch POE o POE Injector (non fornito)
- Batteria interna per funzionamento in mancanza di alimentazione per 8 ore

### OPZIONI

- Modem UMTS USB interno

### INTEGRAZIONI

Perfettamente integrato con Presenze.net di INAZ, tramite IFK Talk. Facile integrazione con tutti i sistemi di Rilevazione Presenze esistenti sul mercato.

A norma con le disposizioni legali sulla privacy con riferimento alle modalità e condizioni di impiego previste dalle Linee guida in materia di trattamento di dati personale di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati – Deliberazione n.53 del 23/11/2006 del Garante per la Privacy e con i provvedimenti specifici in materia di biometria per la rilevazione presenze emanati dal Garante per la Privacy a cui si rimanda per ulteriori approfondimenti - www.garanteprivacy.it

**PER SAPERNE DI PIU'**
vai su www.inaz.it
oppure chiedi al tuo agente INAZ di zona

**INAZ srl** Viale Monza 268, 20128 Milano Tel. 02.27.71.81 marketing@inaz.it

Progettazione e Realizzazione Apparecchiature Elettroniche

Arluno, 15 Giugno 2019

# Algoritmo BIOMETRICO terminali

Technodrive utilizza algoritmi unidirezionali biometrici, in grado di convertire un'immagine in un blocco dati criptato.
Subito dopo la creazione del blocco dati criptato, l'immagine viene rimossa.
**Non e' possibile** convertire il blocco dati criptato in immagine.
Quando il terminale e' configurato in modalita' Mifare, durante la registrazione delle impronte, il blocco dati criptato viene scritto direttamente sul supporto Mifare senza lasciare alcuna traccia dello stesso nel terminale, rendendo quindi impossibile qualsiasi divulgazione del dato biometrico nel database locale del terminale e via rete.
Quando il dipendente appone il badge ed il dito per la varifica, il terminale trasmette e memorizza unicamente matricola, data e ora.

**TECHNODRIVE Srl** -Via E.Ferrari, 7
20010 Arluno (MI) Tel. 02/903.77.887
Sede Legale : Via E.Ferrari, 7 20010 Arluno (MI)
Cod.Fisc. e P IVA 13384950153 R.E.A. n. 1645258 Capitale Sociale 10.000 Euro int. vers.