Installazione di un sistema di rilevazione della presenza in servizio dei dipendenti mediante lettura dell'impronta digitale.

A seguito delle vicende giudiziarie che hanno interessato numerosi dipendenti e che hanno avuto un risalto mediatico nazionale, ingenerando discredito per l'Azienda, è stata proposta all'Autorità Garante per la Privacy specifica istanza di verifica preliminare in relazione all'installazione di un sistema di lettura di dati biometrici mediante identificazione dell'impronta digitale, per la finalità di garantire la sicurezza degli accessi e la prevenzione dall'uso fraudolento dei tesserini magnetici, oltre che contrastare il fenomeno dell'assenteismo.

Nel febbraio del 2017 l'Azienda è stata autorizzata dall'Autorità Garante per la protezione dei dati personali all'installazione di tale sistema.

L' istanza, infatti, si è resa necessaria in quanto i sistemi di rilevazione elettronica (basati sull'utilizzo del badge marcatempo) e di verifica online della presenza dei dipendenti si sono rivelati inefficaci; impossibile inoltre il ricorso ad altri sistemi di controllo delle entrate (es. tornelli o porte elettrocomandate ad accesso controllato) per la toponomastica delle sedi ospedaliere e per la necessità del personale di spostarsi frequentemente da un reparto ad un altro.

Il sistema di rilevazione biometrica è stato attuato nell'ASL di Caserta in maniera assolutamente conforme alle prescrizioni fornite dall'Autorità Garante. (Si allega autorizzazione dell'Autorità Garante)

L'attivazione della rilevazione dei dati biometrici ha comportato :

1- Attivazione di una specifica indagine tramite MEPA per acquisire una prima fornitura di lettori Badge con le relative schede magnetiche .
2·L'avvio della sperimentazione nella sede centrale dell'ASL con l'acquisizione dei dati biometrici di 208 unità (6 Aprile 2017)
3- La successiva estensione a tutti i dipendenti del distretto 12 nelle varie sedi (30 Maggio 2017)
4- L'estensione al personale del Dipartimento di Prevenzione -Sede di Caserta (1/6/2017)
5- L'estensione al personale del Dipartimento di Salute Mentale -Sede di Caserta (5/6/2017)
6- L'attivazione del nuovo sistema nei PPOO dì Marcianise e Maddaloni (1 settembre 2017)
7 - L'attivazione nel Presidio Ospedaliero di S Maria CV (1 settembre 2017)
8- L'attivazione nel Presidio Ospedaliero di Piedimonte Matese (1 Settembre 2017)
9- L'attivazione nel Presidio Ospedaliero di S Felice a C (I Dicembre 2017)
10- L'attivazione nel PO S Rocco di Sessa Aurunca dal 2 Gennaio 2018.
11- Si procederà all'attivazione presso il PO S G Moscati di Aversa appena disponibili i rilevatori biometrici
12- Nel corso del 2018 sarà gradualmente estesa la procedura a tutte le strutture distrettuali e dipartimentali.

Nel 2017 sono stati rilasciati inuovi Badge ed attivata la rilevazione ·dei dati biometrici per 2.091 dipendenti e 127 personale extra con una copertura che si avvicina al 40% della dotazione complessiva.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

UNITÀ LAVORO PUBBLICO E PRIVATO

ASL Caserta
Via Unità d'Italia, 28
81100 – Caserta (CE)

Pec: *direzionegenerale@pec.aslcaserta.it*

c. a. Dir. Dr. Michele G. Tari
Dir. Prevenzione Corruzione e
Trasparenza

Pec: *michele.tari@pec.aslcaserta1.it*

ULPP/DC/113208-1/

Oggetto: trattamento di dati biometrici di dipendenti connesso all'installazione di un sistema di rilevazione della presenza in servizio mediante lettura dell'impronta digitale. Richiesta di verifica preliminare ai sensi dell'art. 17 del decreto legislativo 30 giugno 2003, n. 196 recante il *"Codice in materia di protezione dei dati personali"*.

1. Si fa riferimento all'istanza di verifica preliminare presentata dall'Azienda Sanitaria Locale di Caserta in relazione all'installazione di un sistema di lettura di dati biometrici mediante identificazione dell'impronta digitale, per la finalità di garantire la sicurezza degli accessi e la prevenzione dall'uso fraudolento dei tesserini magnetici, oltre che contrastare il fenomeno dell'assenteismo (istanza del 24 novembre 2016).

Alla luce della documentazione disponibile e delle dichiarazioni rese dal titolare del trattamento, emerge quanto segue:

a) l'Azienda è stata oggetto, fin dal dicembre 2012, di indagini da parte della Procura della Repubblica presso il Tribunale di Santa Maria Capua Vetere e di Napoli Nord, che hanno interessato centinaia di dipendenti per ipotesi di reato quali truffa aggravata ai danni dello Stato (art. 640 c.p.) e false attestazioni o certificazioni nell'utilizzo del badge da parte dei dipendenti pubblici (art. 55-quinquies, d.lg. n. 165/2001);

b) la vicenda - con il coinvolgimento in un'indagine giudiziaria di larga parte dei dipendenti dell'Azienda - ha avuto e tutt'ora ha risonanza sulla stampa locale e nazionale e sui più diffusi mezzi di comunicazione di massa (ad esempio, sul web), ingenerando "allarme sociale" e "discredito" per l'Azienda (cfr. istanza cit., pag. 1);
c) i ripetuti e concreti episodi di violazione dei doveri d'ufficio da parte dei dipendenti ingenerano nell'amministrazione un fondato timore della loro perpetrazione in futuro, considerando la specifica realtà lavorativa e l'elevato numero di lavoratori coinvolti;
d) i sistemi di rilevazione elettronica (basati sull'utilizzo del *badge* marcatempo) e di verifica *on line* della presenza dei dipendenti si sono rivelati inefficaci, anche alla luce dell'azione sanzionatoria finora esercitata, nonché delle oggettive difficoltà del Direttore della Struttura, nell'esercizio dei propri compiti di vigilanza, essendo occupato per larga parte del tempo in servizio nell'attività medica o chirurgica (cfr. istanza cit., pag. 2-3);
e) la toponomastica delle sedi ospedaliere e la necessità del personale di spostarsi in maniera frequente da un reparto all'altro, oltre ad un generalizzato e massivo accesso pubblico agli edifici, impediscono in concreto la possibilità di collocare dei sistemi per il passaggio di una persona per volta (cd. *tornelli*) o di porte elettrocomandate ad accesso controllato (cfr. istanza cit., pag. 3);
f) la rilevazione biometrica, strumento integrativo rispetto alle misure finora adottate dall'Azienda (cfr. istanza cit., p. 4), sarebbe finalizzata a contrastare il fenomeno dell'assenteismo (*"riscontrare con certezza la prestazione lavorativa del dipendente"*) e per avere certezza della corrispondenza tra timbratura e presenza in servizio (cfr. istanza cit., pag. 4) nonché per *"tutelare la salute pubblica come fondamentale diritto dell'individuo e interesse della collettività"* e che assurge a bene giuridico di importanza prioritaria (cfr. istanza, p. 1-2);

2. In relazione alle caratteristiche del sistema ed agli adempimenti giuridici da adottare l'Azienda ha rappresentato che:

a. si provvederà a fornire idonea informativa ai dipendenti, in accordo a quanto disposto all'art. 13 del Codice della privacy;
b. nella fase di registrazione (*enrollment*) il dato biometrico non sarà conservato *"(se non per il tempo necessario all'elaborazione – un paio di secondi)"* in alcun database, ricorrendo ad un'immediata trasformazione della stessa in una striga di bits crittografati che viene memorizzata all'interno di una *smart card* assegnata ad ogni dipendente (cfr. istanza cit., p. 6);
c. il processo di trasformazione dell'immagine dell'impronta digitale in una stringa di bits crittografati è irreversibile, *"in quanto non è possibile in alcun modo ottenere l'immagine dell'impronta a partire dalla stringa di bits*

("template") memorizzata sulla smart card data in uso e custodia al dipendente" (nota cit., p. 6);

d. al momento della rilevazione della presenza il sensore elabora l'immagine dell'impronta ottenendo la stringa dei caratteri crittografati (*template*) relativa che confronta con quella registrata su un tessera *smart card* dotata di microchip cui è preventivamente associato un numero di matricola. In caso di riscontro positivo verranno trasmesse al sistema centrale solo le informazioni di timbratura (matricola, data e ora, causale);
e. il contenuto della stringa di bits sarà protetto da un doppio livello di crittografia: *"un primo livello insito nelle logiche di trasformazione (proprietarie), il secondo livello utilizza la chiave di autenticazione della smart card stessa"* (cfr. istanza cit., p. 6);
f. il sistema preposto rileverà la "vivezza" dell'impronta, la quale verrà verificata *"attraverso i sensori biometrici del lettore DOR30 e dai terminali serie ON"* (cfr. istanza cit., p. 6), in modo da evitare comportamenti fraudolenti (es. copia dell'impronta in silicone);
g. una volta che il dipendente appone sia il badge che il dito sul marcatempo che confronta le informazioni rilevate, questo trasmetterà al sistema centrale, in caso di riscontro positivo, le sole informazioni di timbratura (matricola, data e ora, causale);
h. si eviterà che il dato biometrico venga trasmesso in rete in qualunque forma.

3. Alla luce degli elementi in atti, si osserva preliminarmente che la questione coinvolge la disciplina circa l'utilizzo di dati biometrici, i quali sono *"direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona"*, e che il loro impiego per la specifica finalità di rilevazione delle presenze in servizio non è contemplato tra le ipotesi di trattamento "esonerato" dalla presentazione di istanza di verifica preliminare (cfr. Provvedimento generale prescrittivo in materia di biometria, provv. n. 513 del 12 novembre 2014, in www.garanteprivacy.it., doc. web n. 3556992, punto 4). A tal proposito si rammenta, tuttavia, e come peraltro già noto a codesta azienda, che il Garante si è pronunciato in materia con il provvedimento n. 357 del 15 settembre 2016 (in www.garanteprivacy.it, doc. web n. 5505689, con il quale ha ritenuto il trattamento di dati biometrici per le medesime finalità rappresentate nell'istanza *"lecito e idoneo a soddisfare i principi di necessità e proporzionalità in relazione alla finalità perseguita"*, alla luce delle peculiari circostanze e delle scelte di configurazione del sistema nonché delle modalità di utilizzo che l'Azienda intendeva porre in essere nella situazione specifica (cfr. provv. cit., punto 5).

4. Tutto ciò premesso e considerato, alla luce di quanto dichiarato da codesta Azienda al Garante nelle menzionata nota (anche ai sensi e per gli effetti previsti dall'articolo 168 del Codice), visto il provvedimento n. 357 del 15 settembre 2016 e ritenuto che la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema prospettato dall'istanza in esame corrispondono a quelle già approvate con il predetto provvedimento, il descritto trattamento può aver luogo da parte di codesta azienda sanitaria senza che sia necessario procedere alla verifica preliminare prevista dall'articolo 17 del Codice.

5. Resta fermo che l'Azienda, come peraltro già previsto nel provvedimento adottato in precedenza (cfr. provv. cit., punto 6), prima dell'inizio dei trattamenti, è tenuta in base alla normativa vigente a:

a. effettuare la notificazione al Garante ai sensi dell'articolo 37, comma 1, lett. a), del Codice;
b. fornire ai dipendenti coinvolti un'informativa comprensiva di tutti gli elementi contenuti nell'articolo 13 del Codice (tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione), con riferimento, ovviamente, al trattamento dei dati biometrici, integrando sul punto il modello di informativa trasmesso (cfr., nota 8 giugno 2016);
c. adottare le misure di sicurezza previste dagli articoli 31 e seguenti del Codice al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati;
d. predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 7 e seguenti del Codice.

IL DIRETTORE
(Dott. Mario de Bernart)