GDPR E LINEE GUIDA EUROPEE: LA TUTELA DEI DATI PERSONALI DEGLI INTERESSATI ATTRAVERSO IL CORRETTO UTILIZZO DEI DATI BIOMETRICI

L'art. 4, par. 1, n. 14 del Regolamento UE 2016/679 (GDPR), definisce i **dati biometrici:** "*dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*".
Comunemente i dati biometrici sono quelli relativi a caratteristiche fisiche, fisiologiche o comportamentali di un individuo. Un dato biometrico è, ad esempio, l'impronta digitale usata per sbloccare gli smartphone di ultima generazione, ma anche la conformazione fisica della mano, del volto, dell'iride o della retina, il timbro e la tonalità della voce. La raccolta di tali dati avviene tramite componenti hardware e software, che acquisiscono le informazioni e le analizzano confrontandole con dati acquisiti in precedenza e conservati in un database (non condivisi con il produttore). In tal modo è possibile identificare la persona interessata.

I dati biometrici, però, sono soggetti alla normativa di cui al GDPR solo **se tramite il loro trattamento si può giungere all'identificazione univoca o all'autenticazione di una persona fisica**. Ad esempio, in tema di **riconoscimento facciale**, il Considerando n. 51 del GDPR prevede che: "*Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica*".

Cioè è necessario distinguere tra il vero e proprio **dato biometrico** (il risultato del trattamento, come ad esempio l'impronta del volto o quella digitale) e la **fonte dello stesso** (la fotografia o il dito) che può anche essere oggetto di rilevamento automatizzato delle caratteristiche fisiche di un individuo (nel qual caso diventa dato biometrico). Solo se la finalità è quella di identificare univocamente una persona fisica si possono considerare dati biometrici ai sensi del GDPR. Perché si possa parlare di trattamento di dati biometrici, occorre che la verifica dell'identità sia automatizzata**,** tramite l'ausilio di appositi strumenti software o hardware.

Nel trattare dati personali, soprattutto rientranti nelle categorie di dati particolari (es. stato di salute, appartenenza a partiti politici o sindacati, dati biometrici, ecc…) occorre sempre rispettare i principi cardine del Regolamento ovvero **i principi di liceità, proporzionalità e minimizzazione**, **nonchè dotarsi di misure tecniche ed organizzative adeguate (es. sistemi di cifratura, pseudonimizzazione, ecc…).**

L'uso di questa particolare categoria di dati è da un lato incoraggiato, perché eleva sicuramente il livello di sicurezza dei servizi a seguito di **autenticazione biometrica**, dall'altro occorrono particolari cautele per non configurare rischi o pregiudizi per i soggetti interessati al trattamento, conseguenti all'utilizzo non autorizzata dei dati al di fuori degli scopi originari. Ad esempio, il furto di un dato biometrico derivante da un'impronta digitale può causare un danno notevole in quanto è un sistema di autenticazione univoco e può avere conseguenze per l'intera vita di un individuo. Per tale motivo l'Autorità Garante ha vietato, ad esempio, l'uso centralizzato dei dati biometrici, perché considerato più a rischio per i diritti e le libertà fondamentali degli individui.

Tali dati, infatti, sono dati a trattamento speciale per i quali il GDPR (art. 9, par. 1) **vieta il trattamento se intesi ad identificare in modo univoco una persona fisica**. Alla regola generale seguono, però, una serie di **esenzioni**, che permettono il trattamento dei dati biometrici e nello specifico:
a) se l'interessato ha dato il proprio consenso esplicito al trattamento dei dati personali per uno o più specifici utilizzi (come avviene per il caso dell'autenticazione tramite impronta digitale o della firma

grafometrica in banca), sempre che la legge, nazionale od europea che sia, non vieti comunque il trattamento di tali dati per determinate finalità;

b) se il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo;

c) se l'impiego dei dati biometrici si rende necessario per proteggere un **interesse vitale dell'interessato o di un'altra persona fisica**, quando il soggetto cui i dati si riferiscono si trova in una situazione di incapacità, fisica o giuridica, di prestare direttamente il proprio consenso per tale utilizzo;

d) quando il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua **finalità politiche, filosofiche, religiose o sindacali**, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) quando il trattamento riguarda **dati personali resi manifestamente pubblici dall'interessato**;

f) nell'ambito di un procedimento giudiziario e, in particolare, per accertare, esercitare o difendere un diritto, tanto in sede giudiziaria quanto stragiudiziale;

g) per **motivi di particolare interesse pubblico, previsti dalla legge**, e purché l'impiego di dati biometrici risulti proporzionato alla finalità perseguita, rispetti il diritto alla protezione dei dati e siano comunque previste delle misure di sicurezza appropriate per tutelare i diritti fondamentali e gli interessi del soggetto cui questi dati si riferiscono;

h) quando il trattamento è necessario per **finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;

i) se il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la **protezione da gravi minacce per la salute** a carattere transfrontaliero, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti dell'interessato, in particolare il segreto professionale;

l) quando il trattamento è necessario a **fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**;

m) infine, se il trattamento è effettuato **ad opera o sotto la responsabilità di un professionista soggetto al segreto professionale** per il trattamento di categorie particolari di dati personali relativi alla salute in relazione ad esigenze specifiche, se tale trattamento è effettuato conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

Per tali motivi, anche con riguardo ai dati biometrici, il GDPR si preoccupa di creare una solida struttura di cautele sulla base delle quali consente di procedere all'utilizzo (adeguatamente protetto) di una tipologia di dati la cui possibile applicazione ed utilità è assolutamente evidente.

Alla luce di un utilizzo sempre più frequente di dati biometrici, inoltre, il Comitato Europeo per la protezione dei dati personali (EDPB - European Data Protection Board) ha pubblicato recentemente alcune **Linee Guida n.3/2019** specifiche sul tema.

Qui di seguito si riportano testualmente i **paragrafi n. 77-78-85 dell'art.5 delle Linee Guida EDPB**:

77. Esempio: un Titolare gestisce l'accesso al suo edificio utilizzando un metodo di riconoscimento facciale. Le persone possono utilizzare questo modo di accesso solo se hanno prestato in precedenza un esplicito consenso informato.
Tuttavia, al fine di garantire che nessuno che non abbia precedentemente prestato il proprio consenso sia acquisito, il metodo di riconoscimento facciale dovrebbe essere attivato dall'interessato stesso, ad esempio premendo un pulsante.
Per garantire la liceità del trattamento, il Titolare del trattamento deve sempre offrire un modo alternativo per accedere all'edificio, senza trattamento biometrico, utilizzando magari badge o chiavi.

78. In questi casi in cui vengono generati modelli biometrici i controllori devono assicurare che una volta ottenuto il risultato di una corrispondenza o di una mancata corrispondenza, tutti i modelli intermedi realizzati al volo (con il consenso esplicito e informato dell'interessato) per confrontarli con quelli creati dagli interessati al momento della registrazione, vengano cancellati immediatamente e in modo sicuro. I modelli creati per la registrazione devono essere conservati solo sino alla realizzazione della finalità del trattamento e non devono essere memorizzati o archiviati.

85. Quando il trattamento biometrico viene utilizzato per la finalità di autenticazione, il Titolare del trattamento dei dati deve offrire una soluzione alternativa che non preveda il trattamento biometrico, senza restrizioni o costi aggiuntivi per l'interessato. Questa soluzione alternativa è necessaria anche per le persone che non soddisfano i vincoli del dispositivo biometrico (impossibilità di registrazione o lettura dei dati biometrici, situazione di disabilità che ne rende difficile l'utilizzo, ecc.) e in previsione di indisponibilità del dispositivo biometrico (ad esempio come malfunzionamento del dispositivo), deve essere implementata una "soluzione di backup" per garantire la continuità del servizio proposto, limitato tuttavia a un uso eccezionale.

In questi termini i prodotti **iAccess i985, i985-W, xFace 380, xFace 103 V2, iRis 170, M6, M6-PRO V2, ScanFACE®, Smart Access PRO 30 e Smart Access A 30, soddisfano pienamente i requisiti richiesti dalla normativa in merito alla protezione dei dati personali, poiché non memorizzano le immagini dell'impronta digitale o del volto, ma solo un modello di riferimento anonimo e matematico. Le caratteristiche individuali, biometriche, degli interessati sono vettorizzate in punti univoci e convertite dal terminale in un codice numerico complesso, utilizzando uno specifico algoritmo. L'immagine (ad es. dell'impronta digitale o del volto) non è MAI RIPRODUCIBILE NE' ESPORTABILE DAL TERMINALE, poiché viene memorizzato soltanto un codice numerico. Nel caso in cui un malintenzionato o un soggetto non autorizzato avesse accesso a tali codici, non riuscirebbe a ricondurre la sequenza numerica ad alcun soggetto fisico ovvero non sarebbe possibile il riconoscimento dell'interessato.**

Il GDPR riconosci alcuni diritti a tutti gli interessati come ad es.: revocare il consenso precedentemente prestato nell'ipotesi di uno o più trattamenti per cui sia stato richiesto; ottenere la conferma dell'esistenza di dati personali li riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile e della loro origine, nonché delle finalità, delle modalità di trattamento e della logica applicata in caso di trattamento con strumenti elettronici. In questo caso, l'Azienda dovrà rispondere in modo esaustivo ed immediato, compresa l'eventuale richiesta di cancellazione dei suoi dati, nel momento in cui le informazioni raccolte non fossero più necessarie.

Fra le prescrizioni del GDPR, l'art. 5 par.1 lett. e) specifica che i dati personali sono "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per

le quali sono trattati…". I dati personali dei dipendenti, pertanto, compresi i profili di accesso, possono essere trattati fino al perdurare del rapporto contrattuale di lavoro, mentre altri dati (come ad es. i movimenti) devono essere cancellati, in modo sistematico, manualmente o in automatico.

iAccess, attraverso l'utilizzo del software Time Studio e, più precisamente, attraverso il modulo aggiuntivo Time Pro, consente di eliminare le marcature attraverso la seguente interfaccia: