Documento sottoposto a comsultazione pubblica. Vedi doc. web n. 3127397

VEDI ANCHE

- comunicato stampa del **21 maggio 2014**

- **"Linee guida in tema di riconoscimento biometrico e firma grafometrica"**

[doc. web n. 3132642]

Schema di provvedimento in tema di riconoscimento biometrico e firma grafometrica

Registro dei provvedimenti
n. del

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, di seguito "Codice");

RILEVATO l'elevato numero di notificazioni presentate al Garante relative al trattamento di dati biometrici;

CONSIDERATO che l'evoluzione delle tecnologie biometriche ha generato una significativa diffusione della loro applicazione e ne è prevedibile una ulteriore espansione per il perseguimento di diverse finalità nei più svariati ambiti della società;

ESAMINATE le richieste di verifica preliminare presentate ai sensi dell'art. 17 del Codice in ordine al trattamento dei dati personali effettuati tramite l'utilizzo di tecniche biometriche;

VISTO che, in tale contesto, emerge la necessità di una maggiore sensibilizzazione e attenzione da parte dei titolari e degli interessati agli aspetti che riguardano il corretto trattamento dei dati biometrici;

RITENUTA l'opportunità di rendere disponibile un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale per conformare i trattamenti di dati biometrici alla vigente disciplina sulla protezione dei dati personali e per accrescerne i livelli di sicurezza;

RITENUTO, in ragione della specificità dei dati biometrici, di dovere assoggettare il loro trattamento a un regime generale di obbligatoria comunicazione delle violazioni;

RITENUTA inoltre l'esigenza di individuare, ai sensi dell'art. 17 del Codice, idonee cautele da porre a garanzia degli interessati in relazione ad alcune tipologie di trattamenti di dati biometrici, anche alla luce delle attuali conoscenze tecniche, che potranno essere effettuati senza richiesta di verifica preliminare rivolta al Garante;

VISTE le osservazioni dell'Ufficio formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

1 PREMESSA

L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici è soggetto a una crescente diffusione, in particolare per l'accertamento dell'identità personale nell'ambito dell'erogazione di servizi della società dell'informazione e dell'accesso a banche dati informatizzate, per il controllo degli accessi a locali e aree, per l'attivazione di dispositivi elettromeccanici ed elettronici, anche di uso personale, o di macchinari, nonché per la sottoscrizione di documenti informatici.

Tale diffusione ha suscitato la massima attenzione delle autorità di protezione dati, testimoniata anche dall'elaborazione di pareri da parte del Working Party Article 29 (WP29) che costituiscono un significativo punto di riferimento. I dati biometrici sono infatti dati personali, poiché possono sempre essere considerati come "informazione concernente una persona fisica identificata o identificabile (…)" prendendo in considerazione "l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare

detta persona". Essi rientrano quindi nell'ambito di applicazione del Codice (art. 4, comma 1, lett. b), e le operazioni su essi compiute con strumenti elettronici sono a tutti gli effetti trattamenti nel senso delineato dalla disciplina sulla protezione dei dati personali.

Sono considerati dati biometrici nel presente contesto, coerentemente con i pareri del WP29, i campioni biometrici, i modelli biometrici, i riferimenti biometrici e ogni altro dato ricavato con procedimento informatico da caratteristiche biometriche e che possa essere ricondotto, anche tramite interconnessione ad altre banche dati, a un interessato individuato o individuabile.

2 LINEE-GUIDA IN MATERIA DI TRATTAMENTI BIOMETRICI

Il Garante è intervenuto più volte, a seguito di specifiche richieste di verifica preliminare ai sensi dell'art. 17 del Codice, con provvedimenti che hanno in alcuni casi negato e in altri ammesso, nel rispetto di prescrizioni di natura tecnica od organizzativa, i trattamenti sottoposti alla valutazione dell'Autorità.

Il Garante con il presente provvedimento richiama l'attenzione dei titolari di trattamento, dei soggetti pubblici e privati sull'esigenza che siano osservate, in generale, le disposizioni del Codice e, in particolare, quelle di cui all'art. 17 poiché l'adozione di sistemi biometrici, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e finalità del trattamento, comporta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

A fronte della complessità della materia in rapporto alla disciplina sul trattamento dei dati personali, con l'adozione delle allegate linee-guida, che formano parte integrante del presente provvedimento, il Garante intende fornire un quadro di riferimento unitario sulla cui base i titolari possano orientare le proprie scelte tecnologiche, conformare i trattamenti ai principi di legittimità stabiliti dal Codice, rispettare elevati standard di sicurezza.

Le linee-guida introducono altresì la terminologia essenziale per la descrizione degli aspetti tecnologici, con il ricorso a standard internazionali, e individuano i principali profili di rischio associati al trattamento di dati biometrici.

3 COMUNICAZIONE DI VIOLAZIONE DEI DATI BIOMETRICI

Le peculiari caratteristiche dei dati biometrici, in particolare tenendo conto dei rischi illustrati nelle allegate linee-guida, fanno ritenere necessario assoggettare il loro trattamento all'obbligo di comunicare al Garante le violazioni verificate o temute.

Si richiamano pertanto i titolari all'esigenza di provvedere a informare tempestivamente il Garante in caso di violazioni di dati biometrici destinando le comunicazioni ai recapiti seguenti:

Posta Elettronica Certificata (Pec): protocollo@pec.gpdp.it

Posta elettronica ordinaria: garante@gpdp.it

4 TRATTAMENTI DI DATI BIOMETRICI PER I QUALI NON E' NECESSARIO PRESENTARE ISTANZA DI VERIFICA PRELIMINARE EX ART. 17 DEL CODICE

I dati biometrici sono, per loro natura, direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona, richiedendo particolari cautele in caso di loro trattamento. Pertanto, in considerazione di tali peculiarità, si ritiene necessario prevedere l'obbligo per i titolari di trattamenti biometrici di presentare istanza di verifica preliminare affinché il Garante prescriva, ove opportuno, misure ed accorgimenti per consentire il corretto utilizzo di dati così delicati.

Sulla base dell'esperienza maturata, il Garante individua con il presente provvedimento talune tipologie di trattamento volte a scopi di riconoscimento biometrico, nella forma di identificazione biometrica o di verifica biometrica, o di sottoscrizione di documenti informatici (firma grafometrica) che, in considerazione delle specifiche finalità perseguite, della tipologia dei dati trattati e delle misure di sicurezza che possono essere concretamente adottate, presentano un livello di rischio ridotto.

In relazione a tali specifiche tipologie di trattamenti non è necessario per i titolari, il cui trattamento di dati biometrici rientri nelle tipologie di seguito specificate, presentare istanza di verifica preliminare ai sensi dell' art. 17, a condizione che vengano adottate tutte le misure e gli accorgimenti tecnici individuati con il presente provvedimento e rispettati tutti i presupposti di legittimità contenuti nel Codice e richiamati nelle allegate linee-guida (con particolare riferimento al capitolo 4 che richiama i principi generali di liceità, finalità, necessità e proporzionalità dei trattamenti, unitamente agli adempimenti giuridici tra i quali l'obbligo di informativa agli interessati e di notificazione al Garante).

Il Garante si riserva di prevedere, alla luce dell'esperienza maturata e dell'evoluzione tecnologica, ulteriori ipotesi di esonero dall'obbligo di verifica preliminare.

Le indicazioni relative al trattamento dei dati biometrici contenute nei precedenti provvedimenti del Garante (si vedano, ad esempio, le linee-guida in materia di trattamento di dati personali per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati e pubblici [doc. web n. 1364939 e n. 1417809]) continuano ad applicarsi in quanto compatibili con le previsioni del presente provvedimento.

Resta inteso che i provvedimenti specifici di verifica preliminare sui quali il Garante ha già espresso le proprie valutazioni non dovranno essere oggetto di ulteriori istanze.

4.1 Autenticazione informatica

La Regola n. 2 del Disciplinare tecnico in materia di misure minime di sicurezza, Allegato B al Codice, stabilisce che le caratteristiche biometriche di incaricati del trattamento possano essere usate come credenziali nell'ambito di una procedura di autenticazione informatica relativa a uno specifico trattamento o a un insieme di trattamenti.

In queste specifiche ipotesi, il titolare è sempre chiamato a valutare attentamente che il trattamento in esame sia proporzionato rispetto alle finalità per le quali i dati biometrici sono raccolti e successivamente trattati, in accordo ai principi di pertinenza e non eccedenza di cui all'art. 11 del Codice.

Per tale motivo, il ricorso a sistemi biometrici basati sull'elaborazione dell'impronta digitale, in alternativa alle misure individuate dalla citata Regola n. 2 (parola d'ordine riservata conosciuta solamente dall'incaricato ovvero dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associata a un codice identificativo o a una parola d'ordine), è considerato lecito se commisurato al rischio incombente sui dati trattati, alla cui protezione la stessa procedura di autenticazione è destinata.

In tali casi, il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare purché sia assicurato il rispetto delle seguenti prescrizioni:

a) Il dispositivo di acquisizione deve avere la capacità di rilevare la c.d. vivezza dell'impronta.

b) La cancellazione dei dati biometrici grezzi e dei campioni biometrici deve aver luogo immediatamente dopo la loro raccolta e trasformazione in modelli biometrici.

c) Il dispositivo per l'acquisizione iniziale e quello per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di lavoro o nei sistemi server impiegati nei trattamenti.

d) Le trasmissioni di dati tra i dispositivi di acquisizione e le postazioni di lavoro o i sistemi server sono rese sicure con l'ausilio di tecniche crittografiche robuste.

e) Nel caso in cui i campioni biometrici o i riferimenti biometrici siano conservati su supporti portatili (smart card o analogo dispositivo sicuro):

i. il supporto deve essere nell'esclusiva disponibilità dell'incaricato;

ii. l'area di memoria in cui sono conservati i dati biometrici è resa accessibile ai soli lettori autorizzati e protetta da accessi non autorizzati;

iii. il campione biometrico o il riferimento biometrico devono essere cifrati con tecniche crittografiche robuste;

iv. il supporto è rilasciato in un unico esemplare e, in caso di cessazione dei diritti di accesso ai sistemi informatici, viene restituito e distrutto con una procedura formalizzata.

f) Nel caso di conservazione del campione o del riferimento biometrico sulla postazione informatica (personal computer) o sul sistema server da proteggere con autenticazione biometrica:

i. è assicurata, tramite idonei sistemi di raccolta dei log, la registrazione degli accessi da parte degli amministratori di sistema alla postazione o al server;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifiche della configurazione delle postazioni informatiche, se non esplicitamente autorizzati;

iii. le postazioni sono protette contro l'azione di malware;

iv. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

v. i riferimenti biometrici sono cifrati con tecniche crittografiche robuste;

vi. i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vii. i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati;

viii. sono previsti meccanismi di cancellazione automatica dei dati, cessati gli scopi per i quali sono stati raccolti e trattati.

g) E' esclusa la realizzazione di archivi biometrici centralizzati.

h) Le organizzazioni dotate di certificazione del sistema di gestione della sicurezza delle informazioni (SGSI) secondo lo standard internazionale ISO/IEC 27001:2006 inseriscono il sistema biometrico nel dominio di certificazione del SGSI e pianificano, verificano e aggiornano le relative misure di sicurezza, dandone evidenza nella documentazione prevista unitamente alla valutazione della necessità e della proporzionalità del trattamento biometrico.

i) Le organizzazioni non dotate di certificazione ISO/IEC 27001:2006 redigono e mantengono aggiornata una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare per conformare il trattamento alle prescrizioni sopra elencate, fornendo una valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione tecnica è conservata per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante. Le misure adottate devono essere periodicamente verificate dando luogo alle eventuali azioni correttive e migliorative.

4.2 Controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi

L'adozione di sistemi biometrici basati sull'elaborazione dell'impronta digitale o della topografia della mano può essere consentita per limitare l'accesso ad aree e locali "sensibili" in cui si renda necessario assicurare elevati e specifici livelli di sicurezza oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati e specificamente addetti alle attività.

In tale contesto rilevano, in particolare:

- le aree destinate allo svolgimento di attività aventi carattere di particolare segretezza, ovvero prestate da personale selezionato e impiegato in specifiche attività che comportano la necessità di trattare informazioni riservate e applicazioni critiche;

- le aree in cui sono conservati oggetti di particolare valore o la cui disponibilità deve essere ristretta a un numero circoscritto di addetti, in quanto un loro utilizzo improprio può determinare una grave e concreta situazione di rischio per la salute e l'incolumità degli stessi o di terzi;

- le aree preposte alla realizzazione o al controllo di processi produttivi pericolosi che richiedono un accesso selezionato da parte di personale particolarmente esperto e qualificato;

- l'utilizzo di apparati e macchinari pericolosi, laddove sia richiesta una particolare destrezza onde scongiurare infortuni e danni a cose o persone.

In questi casi il presupposto di legittimità, che in ambito pubblico è dato dal perseguimento delle finalità istituzionali del titolare, in ambito privato viene individuato nell'istituto del bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice) per cui, in ragione del legittimo interesse perseguito dal titolare, delle prescrizioni imposte dal presente provvedimento e delle finalità connesse a specifiche esigenze di sicurezza, il trattamento può avvenire senza il consenso degli interessati.

In relazione a tali finalità, il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare purché sia assicurato il rispetto delle seguenti prescrizioni:

a) Nel caso di utilizzo delle impronte digitali quale caratteristica biometrica, il dispositivo di acquisizione deve avere la capacità di rilevare la vivezza dell'impronta presentata.

b) Il trattamento deve essere applicato nei confronti del solo personale specificatamente selezionato e abilitato ad accedere alle aree e ai locali in questione o ad utilizzare gli apparati e i macchinari pericolosi.

c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici deve aver luogo immediatamente dopo la loro raccolta e trasformazione in modelli biometrici.

d) Il dispositivo per l'acquisizione iniziale e quello per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di controllo ai varchi di accesso.

e) Le trasmissioni di dati tra i dispositivi di acquisizione e le postazioni di lavoro o le postazioni di controllo sono rese sicure con l'ausilio di tecniche crittografiche robuste.

f) Nel caso di esclusiva conservazione del campione o del riferimento biometrico su supporto portatile (smart card o analogo dispositivo sicuro):

i. il supporto deve essere nella esclusiva disponibilità dell'interessato;

ii. l'area di memoria in cui sono conservati i dati biometrici è accessibile ai soli lettori autorizzati ed è protetta da accessi non autorizzati;

iii. il riferimento biometrico deve essere cifrato con tecniche crittografiche robuste;

iv. il supporto è rilasciato in un unico esemplare e, in caso di cessazione dei diritti di accesso alle aree o di utilizzo dei macchinari, viene restituito e distrutto con una procedura formalizzata.

g) Nel caso di conservazione del campione o del riferimento biometrico su un dispositivo-lettore o una postazione informatica dedicata (controller di varco) dotata di misure di sicurezza di cui alla precedente lettera f):

i. è assicurata la registrazione degli accessi alla postazione da parte degli amministratori di sistema, tramite idonei sistemi di raccolta dei log;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche, se non esplicitamente autorizzati;

iii. i sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati;

iv. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

v. il riferimento biometrico deve essere cifrato con tecniche crittografiche robuste;

vi. i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vii. i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati;

viii. sono previsti meccanismi di cancellazione automatica dei dati, cessati gli scopi per i quali sono stati raccolti e trattati.

h) E' esclusa la realizzazione di archivi biometrici centralizzati.

i) Le organizzazioni dotate di certificazione del sistema di gestione della sicurezza delle informazioni (SGSI) secondo lo standard internazionale ISO/IEC 27001:2006 inseriscono il sistema biometrico nel dominio di certificazione del SGSI e pianificano, verificano e aggiornano le relative misure di sicurezza, dandone evidenza nella documentazione prevista unitamente a una valutazione della necessità e della proporzionalità del trattamento biometrico.

j) Le organizzazioni non dotate di certificazione ISO/IEC 27001:2006 redigono e mantengono aggiornata una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare per conformare il trattamento alle prescrizioni sopra elencate, fornendo una valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione tecnica è conservata per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante. Le misure adottate devono essere periodicamente verificate dando luogo alle eventuali azioni correttive e migliorative.

4.3 Uso dell'impronta digitale o della topografia della mano a scopi facilitativi

Le tecniche biometriche possono anche prestarsi a essere utilizzate per consentire, regolare e semplificare l'accesso fisico di utenti ad aree fisiche in ambito pubblico (es. biblioteche) o privato (es. palestre o aree aeroportuali riservate) o a servizi (es. apertura di cassette di sicurezza o accesso a caveau bancari).

In questi casi il presupposto di legittimità del trattamento dei dati biometrici è dato dal consenso effettivamente libero degli interessati ovvero, in ambito pubblico, dal perseguimento delle finalità istituzionali del titolare e dal fatto che dovranno essere assicurati agevoli sistemi alternativi di accesso non basati su dati biometrici.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare purché sia assicurato il rispetto delle seguenti prescrizioni:

a) La cancellazione dei dati biometrici grezzi e dei campioni biometrici deve aver luogo immediatamente dopo la loro raccolta e trasformazione in modelli biometrici.

b) Il dispositivo per l'acquisizione iniziale e quello per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di controllo o nei dispositivi di acquisizione.

c) Le trasmissioni di dati tra i dispositivi di acquisizione e le altre componenti del sistema biometrico sono rese sicure con l'ausilio di tecniche crittografiche robuste.

d) Nel caso di esclusiva conservazione del riferimento biometrico su supporto portatile (smart card o analogo dispositivo sicuro):

a. il supporto deve essere nella esclusiva disponibilità dell'interessato;

b. l'area di memoria in cui sono conservati i riferimenti biometrici è accessibile ai soli lettori autorizzati ed è protetta da accessi non autorizzati;

c. il riferimento biometrico deve essere cifrato con tecniche crittografiche robuste;

d. il supporto è rilasciato in un unico esemplare e, in caso di cessazione dei diritti di accesso ai sistemi informatici, viene restituito e distrutto con una procedura formalizzata.

e) Nel caso di conservazione del riferimento biometrico su un dispositivo-lettore o su postazioni informatiche:

a. è assicurata la registrazione degli accessi alla postazione da parte degli amministratori di sistema, tramite idonei sistemi di raccolta dei log;

b. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione dei dispositivi o delle postazioni informatiche, se non esplicitamente autorizzati;

c. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

d. il riferimento biometrico deve essere cifrato con tecniche crittografiche robuste;

e. i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrici;

f. i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati.

f) E' esclusa la realizzazione di archivi biometrici centralizzati.

g) Le organizzazioni dotate di certificazione del sistema di gestione della sicurezza delle informazioni (SGSI) secondo lo standard internazionale ISO/IEC 27001:2006 inseriscono il sistema biometrico nel dominio di certificazione del SGSI e pianificano, verificano e aggiornano le relative misure di sicurezza, dandone evidenza nella documentazione prevista.

h) Le organizzazioni non dotate di certificazione ISO/IEC 27001:2006 redigono e mantengono aggiornata una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare per conformare il trattamento alle prescrizioni sopra elencate. Tale relazione tecnica è conservata per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante. Le misure adottate devono essere periodicamente verificate dando luogo alle eventuali azioni correttive e migliorative.

4.4 Sottoscrizione di documenti informatici

Il trattamento di dati biometrici costituiti da informazioni dinamiche associate all'apposizione di una firma autografa, a mano libera, su appositi dispositivi di acquisizione (c.d. tavolette grafometriche o dispositivi tablet di uso generale) è ammesso laddove si utilizzino sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal D.lgs. n. 82/2005 (Codice dell'amministrazione digitale), che non prevedano la conservazione centralizzata di dati biometrici.

L'utilizzo di tali sistemi, da un lato, si giustifica al fine di contrastare eventuali tentativi di frode e il fenomeno dei furti di identità e, dall'altro, allo scopo di rafforzare le garanzie di autenticità, non ripudio e integrità dei documenti informatici sottoscritti, anche in vista di eventuale contenzioso legato al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale in sede giudiziaria.

In tali casi, il titolare può procedere al trattamento senza presentare istanza di verifica preliminare ai sensi dell'art. 17 del Codice, purché sia assicurato il rispetto delle seguenti prescrizioni e limitazioni:

a) Il procedimento di firma deve essere abilitato previa identificazione del firmatario.

b) Devono essere resi disponibili sistemi alternativi di sottoscrizione di semplice utilizzo per l'interessato che non comportino l'utilizzo di dati biometrici.

c) La soluzione di firma elettronica avanzata deve essere certificata secondo la norma ISO/IEC 15408, livello EAL 1 o superiore.

d) La cancellazione dei dati biometrici grezzi e dei campioni biometrici deve aver luogo immediatamente dopo la loro raccolta e trasformazione in modelli biometrici.

e) I modelli grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati in forma cifrata, all'interno dei documenti informatici sottoscritti, tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata e certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. La corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave.

f) La trasmissione dei dati biometrici tra sensore e dispositivi, postazioni informatiche e sistemi server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche.

g) Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.

h) I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.

i) Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), devono essere realizzati idonei sistemi di gestione dei dispositivi mobili (sistemi MDM – Mobile Device Management) per isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).

j) I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).

k) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nei documenti di cui alle lettere l) e m) del presente paragrafo.

l) Le organizzazioni dotate di certificazione del sistema di gestione della sicurezza delle informazioni (SGSI) secondo lo standard internazionale ISO/IEC 27001:2006 inseriscono il sistema biometrico nel dominio di certificazione del SGSI e pianificano, verificano e aggiornano le relative misure di sicurezza, dandone evidenza nella documentazione prevista unitamente a una valutazione della necessità e della proporzionalità del trattamento biometrico.

m) Le organizzazioni non dotate di certificazione ISO/IEC 27001:2006 redigono e mantengono aggiornata una relazione che descrive dettagliatamente gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare per conformare il trattamento alle prescrizioni sopra elencate, fornendo una valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione tecnica è conservata per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante. Le misure adottate devono essere periodicamente verificate dando luogo alle eventuali azioni correttive e migliorative.

TUTTO CIÒ PREMESSO IL GARANTE

1. adotta ai sensi dell'art. 154, comma 1, lettera h) del Codice l'unito documento, recante le "Linee-guida in materia di trattamento di dati biometrici per scopi di autenticazione informatica, di controllo degli accessi e di sottoscrizione di documenti informatici", che forma parte integrante della presente deliberazione, al fine di informare i titolari di trattamento, i produttori di tecnologie biometriche, i fornitori di servizi e gli interessati sui diversi aspetti connessi alla protezione dei dati personali, ivi compresi quelli relativi alla sicurezza, e sui presupposti di legittimità dei trattamenti dei dati biometrici;

2. stabilisce, ai sensi dell'art. 154, comma 1, lettera c) del Codice, che i titolari di trattamenti biometrici sono tenuti a comunicare tempestivamente al Garante le violazioni dei dati biometrici accertate o temute secondo le modalità di cui al paragrafo 3;

3. individua, nei termini di cui al paragrafo 4, i casi nei quali per i trattamenti dei dati biometrici non è necessario presentare istanza di verifica preliminare, e prescrive ai soggetti che intendano procedere in qualità di titolari a tali trattamenti, ai sensi dell'art. 17 del Codice, di adottare le misure e gli accorgimenti tecnici, organizzativi e procedurali descritti nel medesimo paragrafo, nonché di rispettare i presupposti di legittimità e le indicazioni contenute nelle allegate linee-guida con particolare riferimento al capitolo 4 "Principi generali e adempimenti giuridici";

4. prescrive ai titolari di trattamenti biometrici che non abbiano richiesto la verifica preliminare al Garante:

   a. di adottare al più presto e, comunque, entro e non oltre centottanta giorni decorrenti dalla data di pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana, le misure e gli accorgimenti di cui al paragrafo 4, qualora essi ritengano che i trattamenti siano compresi tra quelli ivi individuati;

   b. di sospendere, entro e non oltre novanta giorni decorrenti dalla data di pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana, i trattamenti qualora non siano compresi nei casi individuati, né siano a essi riconducibili previo adempimento alle predette prescrizioni;

   c. di sottoporre a verifica preliminare, con interpello al Garante ai sensi dell'art. 17 del Codice, i trattamenti sospesi, qualora sia intendimento dei titolari riprenderli successivamente;

5. dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia – Ufficio pubblicazione leggi e decreti – per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma,

IL PRESIDENTE

IL RELATORE

IL SEGRETARIO GENERALE