GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n.]

Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014

Registro dei provvedimenti
n. 513 del 12 novembre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, 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");

VISTO il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato in G.U.U.E. 2014 L 257, p. 73 (cd. Regolamento eIDAS);

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;

VISTE 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;

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 eventuali violazioni;

RITENUTA inoltre l'esigenza di individuare, ai sensi dell'art. 17 del Codice, opportune 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 effettuate 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 per ogni analisi e studio del fenomeno. 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, lettera 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 RICONOSCIMENTO BIOMETRICO E FIRMA GRAFOMETRICA

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.

A fronte della complessità della materia in rapporto alla disciplina sul trattamento dei dati personali, con l'adozione delle "Linee-guida in materia di riconoscimento biometrico e firma grafometrica" (allegato "A"), 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, unitamente ai rischi su di essi incombenti illustrati nelle linee-guida, fanno ritenere necessario assoggettare il loro trattamento, anche in coerenza con le previsioni del Regolamento europeo eIDAS in tema di identificazione, autenticazione e firma elettronica, all'obbligo di comunicare al Garante il verificarsi di violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware…) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione.

A questo fine, entro ventiquattro ore dalla conoscenza del fatto i titolari comunicano all'Autorità tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici o sui dati personali ivi custoditi. Tali comunicazioni devono essere redatte secondo lo schema riportato nell'allegato "B" al presente provvedimento e quindi inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.biometria@pec.gpdp.it .

4. ESONERO DALLA VERIFICA PRELIMINARE DI CUI ALL'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. 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 delle finalità del trattamento, può comportare quindi rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

In ragione di ciò, qualora si intenda provvedere al trattamento di dati biometrici, è necessario presentare al Garante una richiesta di verifica preliminare, ai sensi dell'art. 17 del Codice.

Sulla base dell'esperienza maturata, però, il Garante ha ritenuto di individuare, 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 a loro protezione, presentano un livello di rischio ridotto.

In relazione a tali specifiche tipologie di trattamenti non è quindi necessario per i titolari presentare la predetta istanza, a condizione che vengano adottate tutte le misure e gli accorgimenti tecnici idonei a raggiungere gli obiettivi di sicurezza individuati con il presente provvedimento e siano rispettati i presupposti di legittimità contenuti nel Codice e richiamati nel capitolo 4 delle linee-guida (con particolare riferimento ai principi generali di liceità, finalità, necessità e proporzionalità dei trattamenti, e agli adempimenti giuridici 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.

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. 14178091) continuano ad applicarsi in quanto compatibili con le previsioni del presente provvedimento.

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

I titolari dei trattamenti biometrici in relazione ai quali è previsto l'esonero dalla verifica preliminare, che abbiano già presentato istanza ex art. 17 del Codice alla data di pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana, sono tenuti a comunicare al Garante, entro trenta giorni dalla stessa data, la conformità del trattamento alle prescrizioni ivi contenute ovvero la propria intenzione di conformarvisi. La presentazione della comunicazione comporta il non luogo a provvedere sulle relative istanze.

Le istanze di verifica preliminare in relazione alle quali non sia stata presentata la comunicazione di cui al periodo che precede verranno invece valutate dal Garante secondo le ordinarie procedure.

4.1 Autenticazione informatica

Le caratteristiche biometriche possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici, laddove è richiesta maggior certezza nell'identificazione degli utenti per particolari profili di rischio relativi alle informazioni trattate e alla tipologia di risorse informatiche impiegate. Appartengono a tale ambito, ad esempio, le infrastrutture critiche informatiche di cui al D.M. 9

gennaio 2008 del Ministro dell'interno (G.U. n. 101 del 30 aprile 2008).

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, lettera g), del Codice) per cui, in ragione del legittimo interesse perseguito dal titolare, delle prescrizioni imposte dal presente provvedimento, delle finalità connesse a specifiche esigenze di sicurezza commisurate ai rischi incombenti sui dati o sui sistemi informatici che la procedura di autenticazione è destinata a proteggere, anche tenuto conto delle indicazioni normative in materia di misure minime di sicurezza delle banche dati, il trattamento dei dati biometrici può avvenire senza il consenso degli interessati.

Quindi i titolari sono esonerati dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nell'emissione vocale.

b) Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza.

c) Nel caso di utilizzo dell'emissione vocale, tale caratteristica è utilizzata esclusivamente in combinazione con altri fattori di autenticazione e con accorgimenti che escludano i rischi di utilizzo fraudolento di eventuali registrazioni della voce (prevedendo, per esempio, la ripetizione da parte dell'interessato di parole o frasi proposte nel corso della procedura di riconoscimento).

d) La cancellazione dei dati biometrici grezzi ha luogo immediatamente dopo la loro trasformazione in campioni o in modelli biometrici.

e) I dispositivi per l'acquisizione iniziale (enrolment) e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi oppure integrati nei sistemi informatici che li utilizzano, siano essi postazioni di enrolment ovvero postazioni di lavoro o sistemi server protetti con autenticazione biometrica.

f) Le trasmissioni di dati tra i dispositivi di acquisizione e i sistemi informatici sono rese sicure con l'ausilio di tecniche crittografiche caratterizzate dall'utilizzo di chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

g) Nel caso in cui i riferimenti biometrici siano conservati in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica UNI CEI ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso ai sistemi informatici, è restituito e distrutto con procedura formalizzata;

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. i campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

h) Nel caso di conservazione del campione o del riferimento biometrico sul sistema informatico protetto con autenticazione biometrica:

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

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

iii. i sistemi informatici sono protetti 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 campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

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

vii. i campioni o 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.

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

j) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica UNI CEI ISO/IEC 27001:2005 e successive modificazioni che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

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 ritenuti "sensibili" in cui è 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.

Appartengono a tale ambito, in particolare:

- le aree destinate allo svolgimento di attività aventi carattere di particolare segretezza, ovvero prestate da personale selezionato e impiegato in specifiche mansioni 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 è ristretta a un numero circoscritto di addetti;

- 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, lettera 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 se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nella topografia della mano.

b) Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza.

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

d) I dispositivi per l'acquisizione iniziale e quelli 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 caratterizzate dall'utilizzo di chiavi di cifratura con lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

f) Nel caso di esclusiva conservazione del riferimento biometrico in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica UNI CEI ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso alle aree sensibili, è restituito e distrutto con procedura formalizzata;

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 è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

g) Nel caso di conservazione 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 e):

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 della postazione informatica, 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 è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

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) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica UNI CEI ISO/IEC 27001:2005 e successive modificazioni che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

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. aree aeroportuali riservate) o a servizi.

In questi casi il presupposto di legittimità del trattamento dei dati biometrici è dato dal consenso effettivamente libero degli interessati e dall'utilizzo di sistemi alternativi di accesso non basati su dati biometrici.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nella topografia della mano.

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

c) I dispositivi per l'acquisizione iniziale e quelli 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.

d) 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 con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

e) Nel caso di esclusiva conservazione del riferimento biometrico in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica UNI CEI ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso, è restituito e distrutto con procedura formalizzata;

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

iii. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

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

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 dei dispositivi o delle postazioni informatiche, se non esplicitamente autorizzati;

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

iv. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

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

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

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

h) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto ai suoi fini facilitativi. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica UNI CEI ISO/IEC 27001:2005 e successive modificazioni che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

4.4 Sottoscrizione di documenti informatici

Il trattamento di dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi hardware è ammesso in assenza di verifica preliminare laddove si utilizzino sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" che non prevedono 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, ha lo scopo di rafforzare le garanzie di autenticità 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 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. Il consenso è espresso dall'interessato all'atto di adesione al servizio di firma grafometrica e ha validità, fino alla sua eventuale revoca, per tutti i documenti da sottoscrivere.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni e limitazioni:

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

b) Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.

c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della procedura di sottoscrizione, e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.

d) I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati 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. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di firma grafometrica può conservare in modo completo tale chiave privata. Le modalità di generazione, consegna e conservazione delle chiavi sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1 lettere e) ed f) del d.P.C.M. 22 febbraio 2013.

e) La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

f) 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.

g) 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.

h) Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di 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).

i) 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).

j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, 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 nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1, lettere e) ed f) del d.P.C.M. 22 febbraio 2013.

k) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica UNI CEI ISO/IEC 27001:2005 e successive modificazioni che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

TUTTO CIÒ PREMESSO IL GARANTE

1. adotta ai sensi dell'art. 154, comma 1, lettera h) del Codice l'allegato "A", recante le "Linee-guida in materia di riconoscimento biometrico e firma grafometrica", 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. prescrive, ai sensi dell'art. 154, comma 1, lettera c) del Codice, che i titolari di trattamenti biometrici comunichino al Garante, entro ventiquattro ore dalla conoscenza del fatto, le violazioni dei dati biometrici secondo le modalità di cui al paragrafo 3;

3. individua, nei termini di cui al paragrafo 4, i casi di esonero dalla presentazione di 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 – entro centottanta giorni dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana – le misure e gli accorgimenti di cui al paragrafo 4, qualora i trattamenti siano compresi nei casi di esonero dall'obbligo di verifica preliminare;

ovvero

b. di sospendere – entro il medesimo termine – i trattamenti e di sottoporre gli stessi a verifica preliminare, con interpello al Garante ai sensi dell'art. 17 del Codice;

5. invita i titolari dei trattamenti biometrici compresi nei casi di esonero dall'obbligo di verifica preliminare, i quali abbiano già presentato istanza, tuttora pendente, ex art. 17 del Codice, a comunicare al Garante – entro trenta giorni dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana – la conformità del trattamento alle prescrizioni ivi contenute ovvero la propria intenzione di conformarvisi. La presentazione della comunicazione comporta il non luogo a provvedere sulle relative istanze. Le istanze di verifica preliminare in relazione alle quali non sia stata presentata la comunicazione di cui al

periodo che precede verranno valutate dal Garante secondo le ordinarie procedure;

6. 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, 12 novembre 2014

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Soro