ADEMPIMENTI NORMATIVI PER AVVIAMENTO NUOVO CLIENTE

smartsign

Rev. 26/10/2015

itworking
INNOVAZIONE APPLICATA

ITWorking S.r.l.
Via 23 Settembre 1845, n. 109
47921 Rimini - RN -
P.Iva e C.Fisc. 03951070402
Capitale Sociale € 100.000,00 I.V.
Registro Imprese Rimini R.E.A. 318186

Tel. 0541.742190
Fax 0541.1810211
PEC: itworking@legalmail.it
Mail: info@itworking.it
www.itworking.it

Scopo del documento

La firma grafometrica consiste nell'apposizione di una sottoscrizione autografa su un particolare tablet, in grado di acquisire, non solo l'immagine della firma, ma anche numerosi dati biometrici, quali posizione, velocità e pressione del tratto. Tutti questi dati vengono associati univocamente al documento oggetto di sottoscrizione e cifrati per renderli inutilizzabili in altri documenti.
I dati biometrici, infatti, sono caratteristiche uniche dell'individuo, utilizzabili pertanto per l'autenticazione di un utente, poiché per le loro intrinseche qualità non possono essere dimenticati, passati ad un altro individuo, persi o rubati da un'altra persona.

Il ricorso a queste soluzioni di Firma Elettronica Avanzata deve essere sempre subordinato all'adesione dell'utente, il quale, dopo essere stato identificato ed adeguatamente informato sulle caratteristiche della soluzione di firma grafometrica utilizzata, esprime il proprio consenso, sempre successivamente revocabile.

Il **Codice per il Trattamento dei Dati personali (D.Lgs. 196/2003)** considera il trattamento di dati biometrici un trattamento che presenta rischi particolari ai fini della protezione della protezione della Privacy. Pertanto, la normativa Privacy pone a carico del titolare del trattamento il dovere di adottare non solo i normali adempimenti richiesti dal Codice per il trattamento di qualsiasi dato personale riferibile ad una persona fisica (informativa, consenso, misure di sicurezza), ma altresì ulteriori adempimenti, quali la notificazione al Garante e più specifici accorgimenti in tema di misure di sicurezza.

In caso di Firma Elettronica Avanzata (FEA), oltre a dotarsi di apposita infrastruttura Software/Hardware, occorre rispettare gli adempimenti previsti dalle seguenti disposizioni normative:
- Decreto del Presidente del Consiglio dei Ministri del 22 Febbraio 2013 contenente la Regole Tecniche in materia di Firma Elettronica Avanzata pubblicato in G.U. n. 117 il 21 maggio 2013. Tale decreto è entrato in vigore il 5 giugno 2013. Le Regole Tecniche riportano al Titolo V, dall'articolo 55 al 61, gli obblighi da rispettare per la produzione, l'erogazione e l'adozione del servizio di Firma Elettronica Avanzata.
- Provvedimento del Garante per la protezione dei dati personali del 12 novembre 2014, pubblicato in G.U. n. 280 il 2 dicembre 2014, che espone di adempimenti in tema di biometria e sottoscrizione dei documenti informatici a mezzo firma grafometrica.

Nel presente documento vengono fornite le indicazioni per un corretto avviamento all'adozione e alla rivendita della soluzione di Firma Elettronica Avanzata per essere conformi alle Regole Tecniche in materia di firma elettronica avanzata e agli adempimenti Privacy previsti dal recente Provvedimento del Garante in tema di biometria.

Identificazione del firmatario

Per iniziare ad erogare la soluzione di Firma Elettronica Avanzata occorre **identificare in modo certo l'utente tramite un valido documento di riconoscimento**, la cui copia dovrà essere conservata per almeno vent'anni.

Informativa per accettazione del servizio da parte del cliente e consenso

L'informativa è da considerarsi il primo e più generale degli adempimenti previsti dal Codice per la Protezione dei dati personali, non solo perché ordinariamente deve precedere l'inizio di ogni trattamento, sia nel settore pubblico sia in quello privato, ma soprattutto perché, essa è il presupposto necessario ed indispensabile per ottenere un valido consenso dell'interessato al trattamento dei dati che lo riguardano.

Attraverso l'informativa il soggetto interessato viene quindi posto in grado di esprimere consapevolmente il consenso al trattamento dei propri dati, così come previsto dall'art. 23 del Codice.

Quando si attiva un nuovo cliente, occorre dare adeguata informazione delle condizioni di servizio e raccogliere il consenso attraverso il documento INFORMATIVA SULLA FIRMA ELETTRONICA AVANZATA. ACCETTAZIONE DELLE CONDIZIONI DI SERVIZIO con Informativa Privacy (si veda documento allegato).

Pubblicazione informativa sul sito

Per iniziare ad erogare la soluzione di Firma Elettronica Avanzata occorre pubblicare sul proprio sito la NOTA INFORMATIVA SULLA FIRMA GRAFOMETRICA (si veda documento allegato).

Polizza assicurativa

Ogni soggetto che eroga soluzioni di Firma Elettronica Avanzata deve **dotarsi di un'assicurazione per la responsabilità civile** come richiesto nell'Art. 57 comma 2 del DPCM del 22 febbraio 2013.
Per aderire alla polizza SmartSign occorre compilare un apposito modulo: clicca qui per scaricare il pdf.
Leggi il testo completo del contratto per l'assicurazione SmartSign: clicca qui per scaricare il pdf.

Notificazione preventiva al Garante Privacy

L'art. 37 del Codice Privacy prevede l'obbligo di **effettuare la notificazione al Garante per chi effettua il trattamento di una serie di dati, specificatamente previsti dalla stessa norma, in quanto ritenuti suscettibili di recare pregiudizio ai diritti ed alle libertà dell'interessato**; in particolare, il comma 1, lettera a) prevede l'obbligo di notificazione per il trattamento di dati biometrici.

La notificazione consiste in una dichiarazione con la quale il soggetto, titolare del trattamento, rende noto al Garante l'esistenza di un'attività di raccolta ed utilizzazione dei dati elencati nell'art. 37 del codice. La notificazione va effettuata prima che inizi il trattamento, ed una sola volta, indipendentemente dalla durata e dal numero di operazioni di trattamento del medesimo tipo di dati che si effettua. Una nuova notificazione sarà necessaria solo prima che cessi definitivamente l'attività di trattamento, oppure prima di apportare al trattamento delle modifiche ad uno degli elementi da indicare nella notificazione stessa.
Tutte le notificazioni trasmesse al Garante vengono inserite in un registro pubblico consultabile gratuitamente da tutti on-line.

La notificazione deve essere trasmessa dal titolare al Garante esclusivamente in via telematica, tramite la procedura presente nel sito www.garanteprivacy.it, la quale prevede la compilazione di una serie di form dove riportare i dati del titolare, informazioni relative alle categorie di dati trattati, alle categorie di interessati cui si riferiscono i dati, alle finalità, alle modalità di trattamento, all'ambito di comunicazione dei dati.

Terminata la compilazione di tutti i campi, il Garante invierà all'indirizzo di posta elettronica indicato dal notificante un messaggio di conferma del ricevimento della notificazione che attesta il buon esito della procedura. Ogni notificazione inviata al Garante (prima notificazione, modifica o cessazione del trattamento) dovrà essere accompagnata dal pagamento dei diritti di segreteria, il cui importo è fissato in euro 150,00.

Per perfezionare la notificazione è poi necessario sottoscriverla con firma digitale (art. 10, comma 3, d.P.R. n. 445/2000) prima della trasmissione telematica.

Si veda in allegato, come esempio, l'esito della notifica ITWorking al Garante.

Adozione di idonee misure di sicurezza

Il trattamento di dati personali (dati direttamente o indirettamente identificativi di persone fisiche), è consentito a condizione che siano rispettate le misure di sicurezza indicate dal D. Lgs. 196/2003.
Tali misure si distinguono in: **idonee e preventive** (indicate dall'art. 31 del Codice) e **minime** (individuate dagli artt. 33-34 e 35.

Le misure idonee e preventive sono quelle che il titolare del trattamento pone in essere al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
Le misure minime sono invece espressamente indicate dagli artt. 34 e 35 del D. Lgs.196/2003 e devo essere attuate con le modalità indicate dal Disciplinare Tecnico allegato B) al decreto.

L'art. 34 indica le misure di sicurezza da attuare nel caso di trattamento con strumenti elettronici:
a) Autenticazione informatica
b) Adozione di procedure per la gestione delle credenziali di autenticazione
c) Sistema di autorizzazione
d) Protezione degli strumenti elettronici e dei dati
e) Salvataggio dei dati
f) Conservazione supporti di copia
g) Disaster recovery

Il Provvedimento del Garante Privacy del 12 novembre 2014 prevede l'assolvimento di alcuni adempimenti in tema di sottoscrizione dei documenti informatici a mezzo firma grafometrica:

- la cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo la sottoscrizione del documento;
- 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;
- i sistemi informatici sono protetti contro l'azione di malware e adottano sistemi di firewall. Sono resi disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi;

- i dati biometrici e grafometrici vanno memorizzati all'interno di documenti informatici in forma cifrata tramite sistemi di crittografia a chiave pubblica. Ai fini della sicurezza e integrità del dato, la corrispondente chiave privata, frazionabile tra più soggetti, deve essere affidata a un soggetto terzo fiduciario e non può essere conservata in modo completo dal soggetto che eroga il servizio di firma grafometrica.

Relazione tecnica con verifica di controllo almeno annuale

È necessario predisporre una relazione sull'uso dei dati biometrici 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 deve essere conservata agli atti, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante. Il provvedimento indica nel termine di 180 giorni (a partire dalla data di pubblicazione del provvedimento in G.U., il 2 dicembre 2014) la tempistica per cui anche questo adempimento deve essere assolto. I titolari dotati di certificazione ISO 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere tale relazione, integrando la documentazione prodotta nell'ambito della certificazione con la valutazione della necessità e della proporzionalità del trattamento biometrico. Le modalità di generazione, consegna e conservazione delle chiavi devono inoltre essere dettagliate sia nell'informativa resa agli interessati che nella relazione tecnica.

Per maggiori informazioni contattaci allo 0541/742190 o scrivi a commerciale@itworking.it.