Sistema di Firma Grafometrica posta alla base di una soluzione di Firma Elettronica Avanzata, per la sottoscrizione di documenti informatici da parte della clientela

Data ultimo aggiornamento: ***19 ottobre 2015***

Componente metodologica:	Descrizione del servizio di Firma Grafometrica
Nome file documento:	BD Firma grafometrica Parte 1 v01.01-01072015.doc
Classificazione documento:	Riservato
Destinatari:	Strutture organizzative destinatarie della Procedura operativa

Predisposto da:	Alessandro Taddia
Validato da:	
Rivisto da:	
Approvato da:	Tonino Calzolari

Validato Banca da:	Michele Cantatore
Rivisto Banca da:	
Approvato Banca da:	

Versione	01.02	**Data Versione**	19/10/2015
Descrizione modifiche	Seconda versione		
Motivazioni	Suggerimenti Studio Legale Finocchiaro		

1. Premessa 4

2. ALLEGATI 5
"Allegato-1" - Fac simile adesione al servizio FEA, informativa e consenso dell'interessato 5
"Allegato-2" - Provvedimento n. 513 del 12 novembre 2014 e relative linee guida 5

3. DEFINIZIONI 6

4. CARATTERISTICHE DELLA "FEA GRAFOMETRICA" DEL CSE 7
Funzionamento del sistema 7
Caratteristiche della soluzione e misure di sicurezza 9
Accesso ai dati biometrici tramite chiave 'privata' 10
Creazione del certificato e delle chiavi di cifratura dei dati biometrici 11

5. PRINCIPI GENERALI E ADEMPIMENTI GIURIDICI (cap. 4 DELLE "LINEE-GUIDA" - Allegato "A" al Provvedimento del Garante per la protezione dei dati personali del 12/11/2014) 13
Liceità (par. 4.1 LINEE-GUIDA) 13
Necessità (par. 4.2 LINEE-GUIDA) 13
Finalità (par. 4.3 LINEE-GUIDA) 15
Proporzionalità (par. 4.4 LINEE-GUIDA) 15
Informativa (par. 4.5.1 LINEE-GUIDA) 16
Notificazione (par. 4.5.2 LINEE-GUIDA) 16
Verifica preliminare (4.5.3 LINEE-GUIDA - Allegato A) 17

6. REQUISITI PER L'ESONERO DALL'OBBLIGO DI PRESENTAZIONE DELLA VERIFICA PRELIMINARE 19

7. RIFERIMENTI NORMATIVI 23

1. PREMESSA

CSE propone alle Banche Clienti un servizio di firma elettronica avanzata basata su tecniche grafometriche (d'ora innanzi "FEA grafometrica"), per la sottoscrizione, da parte della clientela finale, di disposizioni di sportello, contratti e altra documentazione bancaria.

Le finalità della soluzione proposta sono quelle di migliorare la qualità dei servizi, di semplificare i processi di interazione tra la Banca e i propri clienti, nonché di ridurre la carta scambiata nei processi operativi posti in essere.

Il presente documento costituisce parte integrante della "*Relazione sugli aspetti tecnici e organizzativi delle misure messe in atto"*, richiesta dal parag. 4.4 – lettera k) del Provvedimento del Garante per la Protezione dei Dati Personali, del 12 Novembre 2014. Il documento completo è disponibile presso CSE.

Sono parti integranti del sistema di gestione della "FEA grafometrica" le seguenti procedure :

- BD: servizio preposto alla gestione della firma;
- BA: Sportello;
- IC: Vendita Prodotti.
- SR: ambiente di gestione delle credenziali di accesso e delle relative abilitazioni;
- CS: ambiente che contiene il software di conservazione;
- DN: sistema documentale CSE, che contiene i documenti.

Si evidenzia che, nel 2013, le caratteristiche tecniche e funzionali della soluzione di "FEA grafometrica" del CSE hanno ottenuto parere di conformità da un autorevole studio legale specializzato in digitalizzazione e firme elettroniche.

2. ALLEGATI

Il presente documento comprende i seguenti allegati:

"Allegato-1" - Fac simile adesione al servizio FEA, informativa e consenso dell'interessato



Extrabanca_adesion
e al servizio FEA - int

"Allegato-2" - Provvedimento n. 513 del 12 novembre 2014 e relative linee guida



Provvedimento 513
del 12 11 2014.pdf



Linee guida allegate
al Provvedimento gen

3. DEFINIZIONI

Termine o acronimo	***Significato***
Certification Authority	Autorità accreditata (INTESA S.p.A.) che fornisce certificati qualificati di firma e di cifratura, fornisce inoltre servizi di certificazione delle firme elettroniche qualificate e altri servizi connessi quali, ad esempio, la validazione temporale con rilascio di marca temporale.
Documento Informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Firma elettronica Avanzata	E' un particolare tipo di firma elettronica che, allegando oppure connettendo un insieme di dati in forma elettronica ad un documento informatico, garantisce integrità, autenticità del documento sottoscritto e controllo esclusivo dello strumento di firma.
Hash	Funzione che prende in input una stringa di lunghezza variabile e ritorna una stringa di lunghezza fissa.
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad un documento informatico.
SHA-256	Funzione di hash crittografico che produce un'impronta del documento di 256 bit .

Non sono riportati i significati di alcuni acronimi e termini specifici di uso comune.

4. CARATTERISTICHE DELLA "FEA GRAFOMETRICA" DEL CSE

Funzionamento del sistema

La soluzione, sviluppata da CSE in collaborazione con Intesa SpA (gruppo IBM), prevede, alla base del sistema di Firma Elettronica Avanzata, la raccolta dell'immagine della firma e delle caratteristiche di apposizione della stessa da parte dell'interessato, quali:

- pressione;
- accelerazione;
- velocità;
- inclinazione della penna;
- movimenti aerei.

La codifica relativa a questi ultimi elementi, considerati dalla normativa Privacy come dati "biometrici(*)" dell'interessato, è memorizzata in modo criptato unitamente al documento e protetta da ogni trattamento non richiesto.

Risulta evidente che il campione di dati raccolti non consente, al pari della firma autografa, un'identificazione assoluta dell'interessato; sono quindi necessarie ed invariate le consuete attività, da parte dell'incaricato della Banca, di identificazione del cliente.

(*) DEFINIZIONE di DATI BIOMETRICI

"*proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità*"

Il flusso del processo di firma può essere sintetizzato nei seguenti passaggi:

1) Il Cliente si presenta in filiale (oppure è contattato da un Agente/Promotore) per eseguire un'operazione (ad es. una disposizione allo sportello oppure l'apertura di un nuovo rapporto) che richiede la firma di un documento;

2) l'Addetto della Banca (operatore di filiale o Agente/Promotore) identifica il Cliente nelle consuete modalità, procedendo poi secondo la normale operatività;

3) l'Addetto della Banca, qualora il Cliente non abbia mai utilizzato il nuovo servizio di firma, lo informa della possibilità di attivarlo, fornendone termini e condizioni. Quindi innesca la generazione del modulo di adesione e di integrazione dell'informativa sul trattamento dei dati personali. Qualora il Cliente sottoscriva l'adesione e presti consenso al nuovo trattamento, si procede con il passo successivo;

4) l'immagine del documento generato dal sistema informativo (o i suoi dati essenziali) è visualizzabile dal Cliente sul tablet (oppure su uno schermo);

5) l'Addetto della Banca evidenzia il punto di firma (anche più di uno), quindi il Cliente procede apponendo la firma sul tablet, mediante apposita penna. Prima di firmare il Cliente può navigare il documento e leggerne il contenuto. Dopo l'apposizione della firma, sul tablet (o sullo schermo) è visualizzabile il documento comprensivo dell'immagine della firma;

6) il tablet acquisisce l'immagine della firma e i dati biometrici (velocità, pressione, inclinazione, accelerazione e movimenti aerei) ad essa associati. L'abbinamento dei dati genera una Firma Grafometrica non riproducibile da persona diversa dal firmatario;

7) il tablet, man mano che acquisisce i dati, li protegge con chiave di cifratura (protezione nella tratta tablet→pc) e li inoltra al client;

8) il driver del tablet, presente sul client, decifra (grazie alla chiave preconcordata) i dati biometrici ricevuti, i quali vengono poi legati indissolubilmente all'impronta informatica (hash) del documento. Se previsto, anche l'Addetto della Banca appone la propria firma (anche più di una), secondo le medesime modalità del Cliente;

9) l'intero pacchetto (dati biometrici ed hash del documento) è protetto con la chiave pubblica di cifratura nota al software applicativo (client), al fine di impedirne il successivo uso fraudolento. La chiave pubblica, la relativa chiave privata ed il certificato ad esse associato vengono generati da Intesa SpA, in qualità di Certification Authority;

10) il documento (arricchito con il pacchetto cifrato contenente i dati biometrici e l'hash) viene poi definitivamente "sigillato" con l'apposizione della firma elettronica associata alla Banca, al fine di garantire che il documento stesso non possa essere manipolato o modificato in un momento successivo, nonché per dimostrarne, in ogni momento, l'integrità. Il documento così ottenuto non può essere successivamente modificato, pena l'invalidità dello stesso. Un'eventuale manomissione sarebbe difatti rilevata facilmente, anche solo con la semplice

lettura del documento tramite *Adobe Reader.* Anche il certificato per la firma elettronica della Banca è emesso dalla C.A. Intesa;

11) qualora il Cliente lo richieda, l'Addetto della Banca provvede alla stampa e consegna di una copia cartacea del documento, ove è visibile l'immagine della firma precedentemente apposta sul tablet. In alternativa, è possibile renderla disponibile sull'internet banking riservato del Cliente (oppure via mail);

12) il documento informatico viene assoggettato al processo di conservazione a norma.

Caratteristiche della soluzione e misure di sicurezza

Il Sistema utilizza tecniche biometriche basate sul rilevamento della dinamica di apposizione della firma autografa (firma grafometrica), per la sottoscrizione di documenti informatici.

I dati biometrici non sono funzionali al riconoscimento biometrico del Cliente, ma sono incorporati all'interno dei documenti informatici per realizzare la soluzione di "firma elettronica avanzata".

Le informazioni biometriche, con l'ausilio di tecniche crittografiche, vengono strettamente associate allo specifico documento informatico, in modo tale da consentire, solo ex-post, lo svolgimento di analisi grafologiche, da parte di un perito calligrafo, sulla genuinità della sottoscrizione, analogamente a quanto avviene con le firme sui documenti cartacei (tipicamente, a seguito di contenzioso contrattuale o di disconoscimento della sottoscrizione).
L'utilizzo della firma grafometrica per la sottoscrizione di documenti, nella soluzione FEA del CSE, **non prevede la creazione di un archivio centralizzato contenente dati biometrici**, perché le caratteristiche delle singole firme sono, volta per volta, acquisite e incorporate, con le opportune protezioni crittografiche, nel documento informatico, poi archiviato nel sistema di gestione documentale CSE e portato in conservazione.
Pertanto, non viene creata alcuna banca dati biometrica.

La creazione del modello biometrico avviene attraverso un processo univoco e non reversibile; non è quindi possibile ricreare il campione biometrico partendo dal modello biometrico. Le dimensioni del modello biometrico sono sufficientemente ampie da garantire un livello di accuratezza adeguato e, al tempo stesso, evitare che il modello possa essere ricostruito o modificato.

Al fine di scongiurare i rischi di furto d'identità:

- i dati biometrici grezzi generati nel corso del procedimento di acquisizione biometrica sono cancellati da aree di memoria temporanea, centrale e secondaria e dal *filesystem* del sistema utilizzato per l'acquisizione, immediatamente dopo la generazione del campione biometrico;
- le trasmissioni dei dati biometrici tra tablet e postazioni informatiche nonché fra queste ultime e i sistemi *server*, sono effettuate su canali di comunicazione resi sicuri mediante l'uso di sistemi crittografici e su canali di comunicazione cifrati:
    - la comunicazione fra tablet e client è protetta tramite l'utilizzo di cifratura "forte", eseguita direttamente dall'*hardware* e dai *driver* del tablet. In particolare, è utilizzato l'algoritmo a chiave simmetrica AES-256 con chiavi randomiche, scambiate in sicurezza tramite algoritmo *Diffie-Hellman*;

  - i dati biometrici vengono cifrati, sul client, utilizzando una chiave di crittografia a 2048 bit, con certificato di 25 anni di durata, emesso da una Certification Authority (Intesa S.p.A.);
  - il client non colloquia direttamente con il server di gestione della firma, bensì con un servizio di *back-end* (server) CSE, il quale a sua volta colloquia con il server di firma: in tal modo, le applicazioni che hanno accesso al server di firma sono sempre autenticate dal sistema di sicurezza CSE;
- i dati biometrici vengono associati indissolubilmente al documento informatico e l'intero *blob* viene protetto con chiave pubblica di cifratura (generata, iniettata e distribuita direttamente da Intesa nella componente software SDK fornita al CSE ed integrata nell'applicazione di gestione del servizio di firma). **La corrispondente chiave privata è stata consegnata da Intesa S.p.A. al CSE (in busta chiusa), il quale ha inserito tale busta in ulteriore busta chiusa sicura e numerata, consegnandola a sua volta ad un notaio di fiducia, per la sua conservazione in luogo sicuro ed idoneo;**
- l'accesso ai dati biometrici del documento è possibile solo tramite la chiave privata di cui sopra ed avviene esclusivamente in caso di contenzioso con il Cliente e a seguito di esplicita richiesta dell'autorità giudiziaria (vedasi specifico paragrafo seguente);
- il sistema informativo CSE prevede l'adozione di misure idonee e accorgimenti tecnici per contrastare i rischi di installazione di *software* e di modifica della configurazione dei server senza le necessarie autorizzazioni, nonché un SGSI complessivo, in grado di assicurare la corretta gestione dei dati trattati e dei sistemi gestiti (vedasi Documento Programmatico per la Sicurezza CSE – nel seguito anche DPS);
- il sistema informativo CSE è protetto contro l'azione di *malware* (ossia *software* creati allo scopo di creare danni più o meno gravi al sistema) e presenta sistemi *firewall* per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati (vedasi allegato 3 del citato DPS).

Accesso ai dati biometrici tramite chiave 'privata'

Solo ed esclusivamente in caso di contenzioso e su richiesta dell'autorità giudiziaria, il CSE (previa riconsegna da parte del notaio) rende disponibile la chiave privata da utilizzare per decifrare i dati grafometrici presenti nel documento, affinché il perito incaricato effettui il confronto con quelli rilasciati, nell'occasione, dal soggetto "interessato".

L'estrazione della chiave dalla busta numerata viene eseguita in presenza dell'ispettore CSE e dell'ispettore della Banca richiedente, verbalizzando puntualmente l'attività.
Al termine dell'estrazione dei dati richiesti, la chiave utilizzata viene depositata nuovamente in un'altra busta sicura e numerata, con firma dei presenti a conferma dell'integrità e della riservatezza del codice utilizzato.

Il perito tecnico incaricato dall'autorità giudiziaria può così procedere alla verifica ex-post delle caratteristiche della firma apposta sul documento.

La verifica in argomento può avvenire tramite specifico software, in grado di stabilire un esito di "vero/falso" in funzione del superamento di una soglia prefissata *(matching score)* tra il "campione" rilasciato nell'occasione dall'interessato e quello in precedenza formato e cifrato all'interno del documento oggetto di disamina nell'ambito del contenzioso con la Banca.

Creazione del certificato e delle chiavi di cifratura dei dati biometrici

La Certification Authority (Intesa S.p.A.) ha approntato una procedura organizzativa ed operativa, di concerto con il produttore della componente software di gestione del sistema di firma (la società austriaca Xyzmo), tale da azzerare ogni rischio di uso improprio del certificato.

La coppia di chiavi di crittografia ed il certificato ad esse associato vengono generati da Intesa S.p.A. (in qualità di Certification Authority): la chiave pubblica viene "iniettata" nella componente del pacchetto client poi rilasciato al CSE e da quest'ultimo integrato nel servizio di firma BD; la chiave privata, invece, viene consegnata al CSE, che si occupa della sua conservazione in luogo sicuro.
Riportiamo in allegato la Certificazione ISO 27001 della Certification Authority Intesa S.P.A.:



BUREAU VERITAS
Certification

Certification
Awarded to

IN.TE.S.A. SpA
CORSO ORBASSANO 367 – 10137 TORINO ITALY

Bureau Veritas Certification certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

Standards

ISO/IEC 27001:2005

Scope of supply

PRODUCTION OF ELECTRONIC SIGNATURE, ADVANCED ELECTRONIC SIGNATURE, ADVANCED ELECTRONIC SIGNATURE BASED ON A QUALIFIED CERTIFICATE AND TRUSTED MAIL SOLUTIONS. DIGITAL AND LEGAL ARCHIVING.

PRODUZIONE DI SOLUZIONI DI FIRMA ELETTRONICA, FIRMA ELETTRONICA AVANZATA, FIRMA ELETTRONICA QUALIFICATA E DI POSTA ELETTRONICA CERTIFICATA.
SERVIZI DI GENERAZIONE/EMISSIONE DI DOCUMENTI ELETTRONICI, ARCHIVIAZIONE DIGITALE E CONSERVAZIONE SOSTITUTIVA A NORMA.

Scope of Applicability – CI0530 Rev. 01 dated 7th December 2012

Certification cycle start date: 17 DECEMBER 2012

Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: 16 DECEMBER 2015

Original Certification date: 17 DECEMBER 2012
File Number: 6028086
Certificate No. IND12.0131U Version 1, Revision Date : 17 DECEMBER 2012

Etienne Casal
Managing Director

UKAS MANAGEMENT SYSTEMS
008

Certification body address: Brandon Place, 169 Borough High Street, London SE1 1LB, United Kingdom
Local office: Bureau Veritas Certification France, 60 Avenue Du General de Gaulle, 92 046 PARIS LA DEFENSE CEDEX

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.

To check this certificate validity please call: +33 (0) 1 78 66 83 89

Riportiamo inoltre la certificazione ISO 27001 ottenuta, nel 2014, dalla società CSE per la conservazione elettronica di documenti informatici:

DNV BUSINESS ASSURANCE

MANAGEMENT SYSTEM CERTIFICATE

Certificato No. / Certificate No. ***163770-2014-AIS-ITA-ACCREDIA***

Si attesta che / This is to certify that

CSE CONSORZIO SERVIZI BANCARI
Società Consortile a Responsabilità Limitata

Via Emilia 272 - 40068 San Lazzaro di Savena (BO) - Italy

è conforme ai requisiti della norma per i sistemi di gestione:
has been found to conform to the management system standard:

UNI CEI ISO/IEC 27001:2014 (ISO/IEC 27001:2013)

Questa Certificazione è valida per il seguente campo applicativo:
This Certificate is valid for the following product or service ranges:

Gestione della sicurezza delle informazioni per la conservazione di documenti informatici * (Settore EA : 33)
*In accordo con la Dichiarazione di Applicabilità, versione 2.00 del 5 Agosto 2014

*Information security management for preservation of digital documents * (Sector EA : 33)*
*In accordance with the Statement of Applicability, version 2.00 of 5th August 2014

Data Prima Emissione/Initial Certification Date:
2014-09-15
Il Certificato è valido fino al:
This Certificate is valid until:
2017-09-15
L'audit è stato eseguito sotto la supervisione di/
The audit has been performed under the supervision of

Michele Tassinari
Lead Auditor

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

SGQ N°003 A PRD N°003 B
SGA N°003 D SSI N°002 G
SCR N°004 F FSM N°001 I

Membro di MLA EA per gli schemi di accreditamento SGQ, SGA, PRD, PRS, ISP e LAB, di MLA IAF per gli schemi di accreditamento SGQ, SGA, SSI, FSM e PRD e di MRA ILAC per gli schemi di accreditamento LAB

Luogo e Data/Place and Date:
Agrate Brianza (MB), 2014-09-15
Per l'Organismo di Certificazione:
For the Certification Body:

Zeno Beltrami
Management Representative

La validità del presente Certificato è subordinata al rispetto delle condizioni contenute nel Contratto di Certificazione.
Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

DNV GL BUSINESS ASSURANCE ITALIA S.R.L. - CENTRO DIREZIONALE COLLEONI - PALAZZO SIRIO – VIA COLLEONI, 9 - 20864 AGRATE BRIANZA (MB) – ITALY – TEL. 039.68 99 905 – WWW.DNVGL.COM.IT

5. PRINCIPI GENERALI E ADEMPIMENTI GIURIDICI (CAP. 4 DELLE "LINEE-GUIDA" - ALLEGATO "A" AL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 12/11/2014)

Per l'attivazione del trattamento dei dati derivati dalla firma grafometrica dell'interessato, è indispensabile aver preventivamente affrontato e risolto i punti, di seguito riportati, espressamente richiesti dalle LINEE-GUIDA IN MATERIA DI RICONOSCIMENTO BIOMETRICO E FIRMA GRAFOMETRICA - Allegato A al Provvedimento del Garante del 12 novembre 2014.

Liceità (par. 4.1 LINEE-GUIDA)

In via prioritaria, occorre verificare che i dati biometrici siano trattati tenendo presenti i diversi presupposti di liceità stabiliti dal Codice in ragione della natura del titolare del trattamento, fermo restando gli ulteriori ed eventuali obblighi di legge e provvedimenti prescrittivi del Garante.
In ambito pubblico, il trattamento dei dati personali è consentito unicamente per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dal Codice in relazione alla specifica tipologia di dati utilizzati, nonché dalla legge e dai regolamenti (artt. 18 e ss.); in tali casi, i soggetti pubblici non operano in base al consenso dell'interessato, a differenza dei soggetti privati ed enti pubblici economici.
Questi ultimi, prima di iniziare il trattamento, devono, di regola, acquisire il consenso informato dell'interessato, che è sempre revocabile e deve essere manifestato in forma libera ed espressa, ossia deve essere scevro da eventuali pressioni o condizionamenti, fermi restando i casi in cui si è in presenza di uno dei presupposti equipollenti (artt. 23 e 24 del Codice). In particolare, il consenso non è richiesto nei casi in cui il Garante, con proprio specifico provvedimento, abbia già operato un cd. bilanciamento di interessi ed abbia ritenuto prevalente il perseguimento di un legittimo interesse del titolare, come in alcune delle ipotesi per le quali l'Autorità ha ritenuto non essere necessaria la richiesta di verifica preliminare ai sensi dell'art. 17 del Codice (es. controllo di accesso fisico ad aree "sensibili" e controllo dell'identità per l'utilizzo di apparati e macchinari pericolosi; v. al riguardo provvedimento generale contestuale all'adozione delle presenti Linee guida).

Prima dell'inizio del trattamento, l'incaricato della Banca Titolare sottopone, al cliente "interessato", l'informativa ai sensi dell'art 13 del "Codice" e la richiesta di espressione del consenso.
Nel contempo, fornisce al cliente la descrizione del servizio, acquisendone l'adesione.

Necessità (par. 4.2 LINEE-GUIDA)

I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. Prima di procedere all'utilizzo di un sistema biometrico, pertanto, occorre valutare se le stesse finalità possano essere perseguite mediante dati anonimi oppure tramite il sistema biometrico ma con modalità tali da permettere l'individuazione dell'interessato solo in caso di necessità (art. 3 del Codice).
In tale quadro, i sistemi biometrici devono essere predisposti, laddove tecnicamente possibile in coerenza con la finalità perseguita, in modo da cancellare immediatamente, e possibilmente in modo automatico, i

dati biometrici e le informazioni a essi correlate in caso di cessazione del trattamento, ferme restando eventuali disposizioni che prevedano una disciplina differente per casi specifici.

L'acquisizione dei dati biometrici (grafometrici), relativi alle caratteristiche delle modalità di firma del cliente, avviene solo ed esclusivamente a fronte:

- dell'adesione del cliente al servizio;
- della presa visione dell'informativa contenente le finalità e le modalità di gestione;
- dell'espressione del consenso per il trattamento dei suoi dati biometrici;
- della richiesta del cliente di svolgere un'operazione (anche l'apertura di un nuovo rapporto).

Il servizio prevede la gestione elettronica dei documenti fin dalla generazione e la loro conservazione a norma.

Oltre alla riduzione dei costi di gestione e di archiviazione, obiettivi della soluzione sono:

-semplicità di archiviazione e di ricerca, nel tempo, dei documenti in formato elettronico;
-possibilità, da parte della clientela, di accedere in autonomia ai documenti elettronici sottoscritti e crearsene un archivio;
-miglioramento degli aspetti di sicurezza (riservatezza, integrità e disponibilità nel tempo) per i dati trattati.

La conservazione di elementi identificativi dell'interessato si giustifica per l'esigenza di verificare l'autenticità della firma a fronte di controversia.

I dati sono comunque cifrati con una chiave pubblica la cui corrispondente chiave privata è conservata, in maniera sicura e protetta, da parte di un notaio di fiducia incaricato dal CSE.

Solo tramite la chiave privata, è possibile, in caso di contenzioso, accedere ai dati biometrici del cliente.

I documenti, comprensivi di 'blog grafometrico', sono conservati dalla Banca per il periodo necessario sulla base delle normative vigenti tempo per tempo, relativamente agli atti scaturenti dalle operazioni bancarie.

Finalità (par. 4.3 LINEE-GUIDA)

I dati oggetto di trattamento per mezzo di sistemi biometrici devono essere raccolti in maniera accurata e trattati per le sole finalità che il titolare intende legittimamente perseguire, previamente indicate nell'informativa che verrà resa agli interessati, e non possono essere utilizzati in altre operazioni di trattamento che siano con queste incompatibili (art. 11, comma 1, lett. a, b, c ed e, del Codice).
In base a tale principio, ad esempio, se la finalità perseguita nel caso concreto è quella di garantire la sicurezza di persone o beni, potrebbero essere utilizzati sistemi biometrici per controllare l'accesso, da parte dei soli dipendenti autorizzati, a luoghi particolarmente pericolosi; gli stessi dati, tuttavia, non possono essere utilizzati a diversi fini come, per esempio, la verifica del rispetto dell'orario di lavoro dei dipendenti.
E ancora, si potrebbero utilizzare dati biometrici per identificare, senza margine di dubbio e in modo da escludere (o ridurre) ipotesi di frode, un soggetto che voglia effettuare operazioni bancarie, ma senza che dagli stessi dati si possano desumere altre informazioni per verificare anche l'accesso in banca del cliente.

La finalità del servizio è la sottoscrizione, con firma elettronica avanzata, di documenti elettronici, con successiva archiviazione e conservazione in forma digitale e la possibilità di verificare ex-post, a fronte di controversia, le caratteristiche relative alle modalità di apposizione della firma.

Quanto sopra allo scopo di escludere o ridurre ipotesi di frode ai danni di un soggetto che voglia effettuare operazioni bancarie, ma senza che dai dati biometrici trattati si possano desumere altre informazioni per verificare anche l'accesso in Banca del cliente.

Altre finalità perseguite sono la riduzione dei costi di gestione e di archiviazione dei documenti sottoscritti, la semplicità di archiviazione e di ricerca dei documenti in formato elettronico, la possibilità per la clientela di accedere in autonomia ai documenti elettronici sottoscritti e crearsene un archivio, il miglioramento degli aspetti di sicurezza (riservatezza, integrità e disponibilità nel tempo) per i dati trattati e la prevenzione delle frodi.

Dette finalità sono comunicate all'interessato nell'integrazione all'informativa allegata all'adesione al servizio (vedasi allegato-1).

Proporzionalità (par. 4.4 LINEE-GUIDA)

Possono essere trattati i soli dati pertinenti e non eccedenti in relazione alle finalità perseguite (art. 11, comma 1, lett. d, del Codice).
Pertanto, il sistema di rilevazione deve essere configurato in modo tale da raccogliere un numero circoscritto di informazioni (principio di minimizzazione), escludendo l'acquisizione di dati ultronei rispetto a quelli necessari per la finalità perseguita nel caso concreto: ad esempio, se la finalità è quella dell'autenticazione informatica, i dati biometrici non devono essere trattati in modo da poter desumere anche informazioni di natura sensibile dell'interessato.
Occorre evitare, se non per motivate ed eccezionali esigenze, di ricorrere a sistemi che impieghino più di una caratteristica biometrica dell'interessato.

Sono trattati solo dati pertinenti e non eccedenti le finalità perseguite.

In particolare, il "Sistema" è configurato in modo tale da raccogliere un numero circoscritto di caratteristiche comportamentali di apposizione della firma da parte dell'interessato, per l'eventuale conferma dell'identificazione del medesimo in caso di contestazione della sottoscrizione del documento, escludendo in ogni caso l'acquisizione di dati ulteriori (anche biometrici) rispetto a quelli necessari per le finalità. I dati biometrici non sono trattati in modo da desumere anche informazioni di natura sensibile dell'interessato.

Informativa (par. 4.5.1 LINEE-GUIDA)

Prima dell'inizio del trattamento (cioè antecedentemente alla fase di enrolment, laddove prevista), il titolare deve fornire agli interessati un'informativa idonea e specifica relativa all'utilizzo dei dati biometrici.
Nell'informativa, contenente tutti gli elementi previsti dall'art. 13 del Codice, occorre puntualizzare, in particolare, la finalità perseguita e la modalità del trattamento (anche enunciando, sia pure sinteticamente, le cautele adottate, i tempi di conservazione dei dati, l'eventuale loro centralizzazione).
L'informativa deve dare adeguata rilevanza alla natura obbligatoria o facoltativa del conferimento dei dati rispetto al perseguimento delle finalità del trattamento. Laddove sia previsto un sistema alternativo ovvero gli interessati non vogliano o non possano, anche in ragione di proprie caratteristiche fisiche, servirsi del sistema di riconoscimento biometrico, oppure successivamente decidano di non usufruirne più, nell'informativa deve essere precisata anche la facoltà di utilizzare modalità diverse per avvalersi comunque del servizio nel cui ambito è prevista una procedura biometrica. Nel caso in cui il dato biometrico sia registrato in un dispositivo posto nell'esclusiva disponibilità dell'interessato, l'informativa dovrà fornire adeguate istruzioni sulla sua corretta custodia e sugli adempimenti connessi ad un eventuale suo smarrimento, sottrazione, malfunzionamento.
Nel caso in cui i sistemi utilizzati in determinate sedi siano potenzialmente idonei al rilevamento di dati biometrici dell'interessato senza la sua cooperazione (come può avvenire in alcuni casi di riconoscimento facciale, vocale o comportamentale), occorre informare gli interessati dando loro la possibilità di scelta relativamente all'accesso a una zona soggetta a tale tipo di controlli biometrici. L'informativa può essere resa mediante apposita segnaletica in prossimità delle aree soggette a rilevamento biometrico o delle postazioni di rilevamento, oppure può essere fornita con altri mezzi prima dell'interazione dell'interessato con il sistema biometrico (es. riconoscimento vocale tramite telefono preceduto da un avviso).
Analogamente, nei casi in cui il trattamento su base biometrica operi in sinergia con un altro sistema (es. videosorveglianza), l'informativa deve evidenziare tale circostanza in maniera chiara e adeguata, anche con le opportune semplificazioni richieste dallo specifico mezzo utilizzato.

CSE ha predisposto un "fac-simile" di integrazione all'informativa già rilasciata dalla Banca al cliente in occasione dell'instaurazione del rapporto, sulla base dei principi e delle indicazioni del Garante.

Notificazione (par. 4.5.2 LINEE-GUIDA)

Il titolare del trattamento dei dati biometrici è tenuto ad effettuare la notificazione al Garante ai sensi degli artt. 37, comma 1, lett. A), e 38, del Codice. In tale ambito, vanno considerati i casi di esonero dall'obbligo di notificazione riguardanti talune categorie di soggetti in ragione delle attività da essi svolte.

Prima di avviare il trattamento dei dati biometrici, la Banca deve verificare se la notifica effettuata in precedenza all'Autorità Garante prevede il trattamento di dati biometrici relativi alla clientela e, nel caso quest'ultimo non fosse contemplato, deve provvedere all'integrazione della notifica.

Verifica preliminare (4.5.3 LINEE-GUIDA - Allegato A)

L'art. 17 del Codice prevede che il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti, a garanzia dell'interessato, rivolti anche "a determinate categorie di titolari o di trattamenti", ove prescritti.

I dati biometrici sono, per loro natura, direttamente e univocamente collegati all'individuo e denotano in generale un'intrinseca, universale e irreversibile relazione tra corpo e identità, per cui è necessario garantire particolari cautele in caso di trattamento.

L'utilizzo di sistemi biometrici rientra, pertanto, tra i trattamenti che presentano rischi specifici e dovrà essere svolto previa richiesta di verifica preliminare al Garante ai sensi 3 Si richiama il Provvedimento relativo ai casi da sottrarre all'obbligo di notificazione, 31 marzo 2004 (in G.U. n. 81 del 6 aprile 2004, doc. web n. 85261); il provvedimento recante "Chiarimenti sui trattamenti da notificare al Garante" 23 aprile 2004 (doc. web n. 993385) ed il provvedimento riguardante le "Notificazioni in ambito sanitario: precisazioni del Garante" 26 aprile 2004 (doc. web n. 996680).

13 dell'art. 17 del Codice. Attraverso la verifica preliminare, che deve essere presentata dal titolare prima dell'inizio del trattamento, il Garante ha il compito di prescrivere, ove necessario, misure e accorgimenti specifici per consentire il corretto utilizzo di dati così delicati nel contesto del trattamento prospettato.

Nella istanza di verifica preliminare il titolare dovrà fornire elementi informativi inerenti l'analisi dei rischi effettuata e le modalità con cui intende garantire il rispetto delle misure di carattere generale, degli adempimenti giuridici e delle misure descritte nel par. 8 delle presenti linee-guida.

In particolare, l'istanza dovrà recare i seguenti elementi informativi:

- *la tipologia di dati biometrici trattati;*
- *il contesto e le specifiche finalità perseguite mediante il sistema biometrico che si*
- *intende installare;*
- *le ragioni in base alle quali si ritengono inidonei rispetto agli scopi perseguiti sistemi alternativi che pongono minori rischi per i diritti e le libertà fondamentali degli interessati;*
- *le modalità di funzionamento del sistema nonché le modalità di acquisizione, utilizzo e archiviazione dei dati biometrici e la durata della loro eventuale conservazione;*
- *l'eventuale idoneità del dato biometrico raccolto a rivelare informazioni relative allo stato di salute degli interessati;*
- *gli eventuali vantaggi per gli interessati e per i titolari del trattamento derivanti dall'utilizzo di dati biometrici;*
- *i rischi individuati e gli accorgimenti tecnici e organizzativi messi in atto per mitigarli;*
- *le modalità di acquisizione del consenso, ove previsto, i sistemi alternativi, il testo dell'informativa.*

Tanto premesso, il Garante – con provvedimento generale contestuale all'adozione delle presenti linee-guida – ha individuato alcune specifiche tipologie di trattamenti in relazione alle quali non ritiene necessaria la presentazione della predetta richiesta di verifica preliminare, a condizione che vengano rispettati i presupposti di legittimità contenuti nel Codice e nelle presenti linee-guida e che vengano adottate tutte le misure e gli accorgimenti tecnici descritti nel medesimo provvedimento. I trattamenti in questione sono:

- *autenticazione informatica;*
- *controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi;*
- *uso delle impronte digitali o della topografia della mano a scopi facilitativi;*
- *sottoscrizione di documenti informatici.*

Come precisato nel successivo capitolo, fermi restando gli adempimenti a carico di ciascuna Banca, si ritiene che la firma grafometrica posta alla base della soluzione di "Firma Elettronica Avanzata" proposta dal CSE possa essere attivata senza obbligo di procedere alla verifica preliminare, in quanto sono rispettati i requisiti imposti dall'Authority, non è previsto un archivio centralizzato dei dati grafometrici e l'accesso ai medesimi, all'interno del singolo documento, può avvenire solo in caso di controversia, su richiesta dell'Autorità Giudiziaria.

6. REQUISITI PER L'ESONERO DALL'OBBLIGO DI PRESENTAZIONE DELLA VERIFICA PRELIMINARE

Con riferimento a quanto prescritto nel parag. 3 del Provvedimento del Garante del 12 Novembre 2014:

> **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 .

CSE ha inserito specifica previsione nel documento "Procedura di gestione degli incidenti", trasmessa alle Banche clienti.

Con riferimento ai requisiti da soddisfare per l'esonero da verifica preliminare al Garante per la protezione dei dati personali (rif. parag. 4.4 del Provvedimento), si riportano nel prosieguo le opportune indicazioni, evidenziando le fattispecie a carico Banca.

a) il procedimento di firma è abilitato previa identificazione del firmatario

Per le specifiche si rimanda alla normativa interna relativa all'identificazione ed adeguata verifica.

b) sono resi disponibili sistemi alternativi di sottoscrizione di semplice utilizzo per l'interessato, che non comportano l'utilizzo di dati biometrici

Occorre consentire al cliente di decidere se utilizzare il sistema di firma autografa su carta o il sistema di "FEA grafometrica". Il sistema CSE permette di stampare il contratto proposto al cliente ed in visione sul tablet/video, per la firma su carta. In seguito il contratto firmato viene scansionato, archiviato e reso disponibile alla visione tramite le procedure CSE. Il cartaceo viene inviato in conservazione presso l'Outsourcer di riferimento Banca.

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;

Al termine della singola operazione, tutti i dati biometrici acquisiti e trattati dal tablet vengono cancellati.

d) i dati 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 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;

I dati biometrici acquisiti sul tablet vengono immediatamente protetti con una chiave di cifratura ed inoltrati al client, senza alcuna conservazione sul dispositivo di raccolta. Subito dopo l'inoltro al client, i dati biometrici vengono indissolubilmente legati all'impronta (hash) del documento, con la chiave pubblica di cifratura.
La chiave privata è conservata in maniera sicura e protetta da parte di un notaio di fiducia incaricato dal CSE.
Le due chiavi e il certificato ad esse associato sono emessi dalla Certification Authority Intesa S.p.A. (dimensione chiavi: 2048 bit).
Le modalità di generazione, consegna e conservazione delle chiavi sono dettagliate nel informativa per gli "interessati" (vedasi allegato-1).

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;

La comunicazione tablet→client è protetta con tecnica di cifratura "forte", tramite chiave randomica scambiata fra il tablet ed il suo driver presente sul client.
Subito dopo l'inoltro al client, i dati biometrici vengono indissolubilmente legati all'impronta (hash) del documento e cifrati insieme a quest'ultima, andando a realizzare quella che, tecnicamente, si definisce come *"document binding"*, ovvero una procedura in grado di dimostrare, in maniera inequivocabile, la correlazione fra documento e firma elettronica. La cifratura dei dati biometrici e dell'impronta del documento avviene tramite chiave pubblica (lunghezza 2048 bit)

emessa (unitamente a quella privata e al certificato ad esse associato) dalla Certification Authority Intesa S.p.A.
La cifratura consente di far sì che nessun dato viaggi mai in chiaro nella tratta tablet→client→server.
Inoltre, l'accesso al server è sempre autenticato, ovvero può essere effettuato esclusivamente da applicazioni integrate nella sicurezza CSE, previo *log-on* dell'utente.

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;

E' esclusa la possibilità di installare software e modificare la configurazione dei dispositivi tablet forniti, a noleggio, dal CSE. Extrabanca è in regime di full outsourcing HD e SW.

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;

Vedasi allegato 3 al Documento Programmatico per la Sicurezza.

h) nel caso di utilizzo 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);

La configurazione dei sistemi "mobili" è gestito direttamente dalla Banca titolare dei dati, tramite che fornisce i tablet in regime di full Ousourcing.

i) il Sistema adotta certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, prevedendo funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi);

Prescrizione a carico Banca.

CSE Utilizza sistemi di identificazione/certificazione dei sistemi client, per impedire l'accesso da sistemi non identificati.
Le procedure e le policy di gestione sono emanate, comunicate al personale incaricato e periodicamente sottoposte a controllo ed eventualmente aggiornate.

La gestione e l'eventuale *wiping* dei dispositivi mobili è, come indicato al punto precedente, in carico alla Banca, eventualmente tramite la società da questa individuata per la gestione 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;

I dati biometrici sono accessibili solo tramite la chiave privata.

Il CSE rende disponibile tale chiave solo ed esclusivamente in caso di contenzioso e su richiesta dell'Autorità Giudiziaria.

Il "fac-simile" di descrizione del servizio ed integrazione dell'informativa, predisposto dal CSE per gli "interessati" (vedasi allegato-1), contiene indicazioni sulle modalità di accesso ai dati biometrici.

k) È predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e 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.

Come indicato in premessa, il presente documento costituisce parte integrante della "*Relazione sugli aspetti tecnici e organizzativi delle misure messe in atto"*, richiesta dal parag. 4.4 – lettera k) del Provvedimento del Garante per la Protezione dei Dati Personali, del 12 Novembre 2014.

Dal 2015 è riportato in allegato al Documento Programmatico per la Sicurezza, unitamente alla scheda tecnica contenente la descrizione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) adottato.

7. RIFERIMENTI NORMATIVI

Di seguito i principali riferimenti normativi.

DPR 445/00	Decreto del Presidente della Repubblica del 28 dicembre 2000, n.445 - "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*. (G.U. n.42 del 20 febbraio 2001)
DLGS 196 30/06/03	Codice in materia di protezione dei dati personali (G.U. n.174 del 29 luglio 2003, suppl. ord.) e relativi provvedimenti/linee guida
DPCM 30/03/2009	Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale, dei documenti informatici. (G.U. n. 129 del 6 Giugno 2009).
DPCM 22/02/2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
DLGS 82 07/03/2005	Decreto Legislativo 7 Marzo 2005, n. 82 - *Codice dell'amministrazione Digitale* (nel seguito indicato semplicemente come CAD), e successive modificazioni. (G.U. n.112 del 16 Maggio 2005)
Deliberazione CNIPA n.45 21/05/2009	Deliberazione CNIPA 21 Maggio 2009 - *Regole per il riconoscimento e la verifica del documento informatico*. (G.U. n.282 del 3/12/2009)
Determinazione commissariale DigitPA N.69/2010 28/07/2010	Modifiche alla Deliberazione 21 maggio 2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante *Regole per il riconoscimento e la verifica del documento informatico*, pubblicata il 3 dicembre 2009 sulla Gazzetta Ufficiale della Repubblica Italiana - Serie generale - n. 282. (G.U. n. 191 del 17/08/2010)
DPCM 10/02/2010	Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza. (G.U. n.98 del 28 Aprile 2010).
DLGS 235 30/12/2010	Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante *Codice dell'amministrazione digitale*, a norma dell'articolo 33 della legge 18 giugno 2009, n.69. (G.U. n.6 del 10/01/2011)

Con riferimento al D.lgs n. 196 del 30 giugno 2003 – "Codice in materia di Protezione dei dati personali", sono presi in considerazione, in particolare, i seguenti articoli:

…….Omississ..

Art. 3. Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

…….….Omississ..

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

……..….Omississ..

Art. 13. Informativa

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

……..….Omississ..

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla
natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.
2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio
del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

……..….Omississ..

Art. 23. Consenso

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.
2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.
3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.
4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:
a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche
richieste dell'interessato;

……..Omississ..

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:
a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica.